Foreigner CA
Énoncé des pratiques de Certification

OID: 2.16.56.1.1.1.7
OID: 2.16.56.1.1.1.7.1
OID: 2.16.56.1.1.1.7.2
OID: 2.16.56.9.1.1.7
OID: 2.16.56.9.1.1.7.1
OID: 2.16.56.9.1.1.7.2

Table des matières

1. INTRODUCTION 5

1.1 AVERTISSEMENT PRELIMINAIRE 5
1.1.1 Entités de confiance régies par le présent CPS 5
1.1.2 Relations entre les entités régies par ce CPS 6
1.2 PORTEE DU PRESENT CPS 7 1.3 LES CERTIFICATS SUR LA CARTE POUR ETRANGER 8 1.4 RELATION ENTRE CE CPS ET D'AUTRES DOCUMENTS 9 1.5 POSITIONNEMENT DU "FOREIGNER CA" DANS LA HIERARCHIE CA 9 1.6 NOM ET IDENTIFICATION DU DOCUMENT 12 1.7 PARTICIPANTS PKI 12
1.7.1 Autorité de certification pour le Foreigner CA 12
1.7.2 Fournisseur de Root Sign 13
1.7.3 Autorité d'enregistrement et autorités d'enregistrement locales 13
1.7.4 Personnalisateur de cartes 14 1.7.5 Initialisateur de cartes 14
1.7.6 Usagers 14
1.7.7 Parties confiantes 15
1.8 UTILISATION DU CERTIFICAT 15 1.9 GESTION ADMINISTRATIVE 15 1.10 DEFINITIONS ET ACRONYMES 15

2. RESPONSABILITES EN MATIERE DE PUBLICATION ET D'ARCHIVAGE 16

2.1 CONTROLE D'ACCES AUX REPERTOIRES 16

3. IDENTIFICATION ET AUTHENTIFICATION 18

3.1 DENOMINATION 18 3.2 VALIDATION DE L'IDENTITE INITIALE 18 3.3 IDENTIFICATION ET AUTHENTIFICATION POUR DES DEMANDES DE RECOMPOSITION (RE-KEY) 18 3.4 IDENTIFICATION ET AUTHENTIFICATION POUR DES DEMANDES DE REVOCATION ET DE SUSPENSION 18

4. EXIGENCES OPERATIONNELLES POSEES AU CYCLE DE VIE D'UN CERTIFICAT 19

4.1 DEMANDE DE CERTIFICAT 19 4.2 TRAITEMENT DE LA DEMANDE DE CERTIFICAT 19 4.3 DELIVRANCE DU CERTIFICAT 19 4.4 ACCEPTATION DU CERTIFICAT 20 4.5 PAIRE DE CLES ET EMPLOI DU CERTIFICAT 20
4.5.1 Droits et obligations de l' étranger 20
4.5.2 Droits et obligations de la partie confiante 20
4.6 RENOUVELLEMENT DU CERTIFICAT 21 4.7 RECOMPOSITION (RE-KEY) 21 4.8 MODIFICATION DU CERTIFICAT 21 4.9 REVOCATION ET SUSPENSION DU CERTIFICAT 21
4.9.1 Durée et fin de la suspension et de la révocation 22
4.10 SERVICES D'ETAT DU CERTIFICAT 22 4.11 DEPOT ET RECUPERATION DE CLES 23

5. CONTROLES ADMINISTRATIFS, OPERATIONNELS ET PHYSIQUES 24

5.1 CONTROLES DE SECURITE PHYSIQUES 24 5.2 CONTROLES DES PROCEDURES 24
5.3 CONTROLES DE SECURITE DU PERSONNEL 25
5.3.1 Qualifications, Expérience, Autorisations 25
5.3.2 Vérifications des antécédents et procédures d'autorisation 25
5.3.3 Besoins et procédures de formation 25 5.3.4 Période et procédures de recyclage 25
5.3.5 Rotation des jobs 26
5.3.6 Sanctions à l'encontre du personnel 26
5.3.7 Contrôle des contractants indépendants 26
5.3.8 Documentation pour la formation initiale et le recyclage 26
5.4 PROCEDURES DE JOURNALISATION D'AUDIT 26 5.5 ARCHIVAGE DES DOSSIERS 27
5.5.1 Types de dossiers 27
5.5.2 Période de conservation 28 5.5.3 Protection des archives 28
5.5.4 Procédures de back up des archives 28 5.5.5 Condition d'horodatage sur les dossiers 28

5.5.6 Collecte des archives 28
5.5.7 Procédures d'obtention et de vérification des informations d'archivage 28
5.6 CHANGEMENT DE CLE 28 5.7 RECUPERATION DE COMPROMISSION ET DE CATASTROPHE 29 5.8 RESILIATION DU CA 29
6. CONTROLES DE SECURITE TECHNIQUE 30
6.1 GENERATION ET INSTALLATION DE LA PAIRE DE CLES 30 6.1.1 Procédure de génération de clé privée CA 30
6.1.2 Génération de la clé CA 30
6.2 REGENERATION ET REINSTALLATION DE LA PAIRE DE CLES 31
6.2.1 Dispositifs de génération de la clé du CA 31
6.2.2 Stockage de la clé privée du CA 31 6.2.3 Distribution de la clé privée du CA 32
6.2.4 Destruction de la clé privée du CA 32
6.3 PROTECTION DE LA CLE PRIVEE ET CONTROLES DU MODULE CRYPTOGRAPHIQUE 32 6.4 AUTRES ASPECTS DE LA GESTION DE LA PAIRE DE CLES 32
6.4.1 Corruption des ressources informatiques, logiciels, et/ou données 33
6.4.2 Révocation de la clé publique du CA 33
6.4.3 Compromission de la clé privée du CA 33
6.5 DONNEES D'ACTIVATION 33 6.6 CONTROLES DE LA SECURITE INFORMATIQUE 33 6.7 CONTROLES DE SECURITE DU CYCLE DE VIE 33 6.8 CONTROLES DE SECURITE DU RESEAU 34
7. CERTIFICAT ET PROFILS CRL 35
7.1 PROFIL DU CERTIFICAT 35 7.1.1 Certificat d'identité 35
7.1.2 Certificat pour signature numérique 36
7.1.3 Certificat "Foreigner CA" 37
7.2 PROFIL CRL 38 7.3 PROFIL OCSP 39
8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 40 9. AUTRES POINTS ET CONSIDERATIONS JURIDIQUES 42
9.1 HONORAIRES 42
9.2 RESPONSABILITE 42
9.2.1 Certificats qualifiés 43
9.2.2 Certificats qui ne peuvent pas être considérés comme des certificats qualifiés 43
9.3 CONFIDENTIALITE DES INFORMATIONS 43 9.3.1 Conditions de divulgation 44
9.3.2 Protection des informations personnelles 44
9.3.3 Droits de propriété intellectuelle 45
9.4 REPRESENTATIONS ET GARANTIES 45 9.4.1 Obligations de l' étranger 45
9.4.2 Obligations de la partie confiante 46
9.4.3 Responsabilité de l' étranger envers les parties confiantes 46
9.4.4 Conditions d'utilisation du centre de demande et du site Web 46
9.4.5 Obligations du CSP 47
9.4.6 Mesure du niveau de service 48
9.4.7 Obligations de la RA (applicables au RRN) 48
9.4.8 Obligations du personnalisateur et de l'initialisateur (CM) 48
9.5 DEGAGEMENTS DE GARANTIE 49
9.5.1 Exclusion de certains éléments de préjudices 49
9.6 DUREE ET RESILIATION 49 9.7 REMARQUES INDIVIDUELLES ET COMMUNICATIONS AVEC LES PARTICIPANTS 49 9.8 CLAUSE CONTRAIGNANTE 49 9.9 AMENDEMENTS 50 9.10 PROCEDURES DE RESOLUTION DES LITIGES 50 9.11 DROIT APPLICABLE 50 9.12 DISPOSITIONS DIVERSES 50
10. LISTE DE DEFINITIONS 51 11. LISTE D'ACRONYMES 55

1. Introduction

1.1 Avertissement préliminaire

Le présent Enoncé des Pratiques de Certification (ci-après abrégée en “CPS” - Certification Practice Statement”) décrit les pratiques de certification applicables aux certificats numériques émis pour les cartes pour étrangers résidant en Belgique (ci-après dénommées “cartes pour étrangers”) par le prestataire de services de certification (ci-après abrégé en CSP) sous l’appellation de “Foreigner CA”.

Ce CPS doit également être considéré comme étant la Police de Certificat (Certificate Policy CP) pour les certificats émis par les autorités de certification “Foreigner CA”.

Par étrangers résidant en Belgique (ci-après dénommés “étrangers”), on entend à la fois les immigrants provenant de l’intérieur et de l’extérieur de l’union Européenne

1.1.1 Entités de confiance régies par le présent CPS

Actuellement, le CSP pour le « Foreigner CA » est la “Société Anonyme CERTIPOST”, dont le siège social est établi au Centre Monnaie à 1000 Bruxelles, engagée à cette fin par les Autorités Fédérales Belges en qualité d’autorité contractante pour le projet eID, dans les termes suivants:

CERTIPOST assume le rôle de prestataire de services de certification (“CSP”) dans le sens de la loi du 9 juillet 2001 (ci-après “la Loi sur la signature électronique”) et de la directive européenne 1999/93.

Le « Foreigner CA » est le nom technique des autorités de certification qui émettent les certificats d’identité et de signature pour la carte pour étranger.

En particulier, CERTIPOST est responsable du “Foreigner CA” en vertu d’un “accord cadre ” daté du 14 novembre 2002 (Réf. RRN 006/2001) conclu entre la s.a. de droit public BELGACOM et les Autorités Fédérales Belges et transféré par BELGACOM à CERTIPOST le 1er juillet 2004, dans lequel Certipost est responsable, en tant qu’agent technique de confiance, de l’infrastructure délivrant les certificats sous la responsabilité d’un CSP, selon un SLA spécifique.

En vertu de cet accord cadre, CERTIPOST accepte de fournir, publier et maintenir les certificats d’identification et les certificats de signature pour les cartes pour étrangers et de fournir des services de confiance liés à ces certificats comme la publication des Listes de Révocation de Certificats (“CRL”), la fourniture de services de validation de certificats en ligne OCSP (“Online Certificate Status Protocol”), des services d’archivage et des services de consultation de certificats. En particulier, les tâches sont limitées à celles visées aux lots 2 et 4 du Cahier Spécial des Charges et à l’ensemble des demandes de changement requis, à l’exclusion du poste 10 du Lot 2 et du poste 9 du Lot 4, tel que décrit dans la BAFO (“Best and Final Offer”) acceptée par l’Autorité Fédérale Belge.

CERTIPOST assume à la fois le rôle de CA (= infrastructure qui délivre des certificats pour le compte d’un CSP, selon un SLA spécifique) et de CSP, sachant que l’Autorité Fédérale Belge sont le CSP responsable du Belgium Root CA, et supporte donc la responsabilité générale pour la délivrance des certificats.

En marge du CSP, d’autres parties sont impliquées dans le projet pour les cartes pour étrangers. Ces parties sont:

1) Les autorités:

L’Autorité d’Enregistrement (“RA”) qui, au nom et pour le compte du CSP, certifie qu’une clé publique donnée appartient à une entité déterminée (par exemple une personne) en délivrant un certificat numérique et en le signant avec sa clé privée. Pour la carte pour étranger le “Registre National”, une administration publique appartenant à l’Autorité Fédérale Belge pour le Service

Public Fédéral Intérieur, assume le rôle de "RA". Le RRN[1] délègue la majeure partie de ses opérations d'enregistrement aux services administratifs locaux de la population dans les administrations communales. Sur la base de ces informations, la RA prie le CA de délivrer un certificat. Le Registre National délègue les opérations d'enregistrement aux services administratifs locaux de la population dans les administrations communales, ce que l'on appelle les Autorités d'Enregistrement Locales ("LRA"). Sur la base de ce processus, la RA prie le CA d'émettre un certificat.

En particulier, la RA est responsable de

(i) l'authentification des étrangers,
(ii) l'enregistrement des données à certifier,
(iii) l'autorisation de délivrer un certificat pour un étranger,
(iv) veiller à ce que les certificats des étrangers soient stockés sur la carte approprié et
(v) veiller à ce que l'étranger reçoive la carte qu'il s'attend à recevoir et active la carte en question uniquement lorsque celle-ci a été attribuée en bonne et due forme au étranger approprié,
(vi) la SRA (Autorité de Suspension et de Révocation) : l'entité qui suspend et/ou révoque les certificats dans le sens de la Loi sur la signature électronique.

2) Le fabricant de cartes (Card Manufacturer):

Le fabricant des cartes ("CM"[2]) est l'entreprise Zetes, engagée à cette fin par l'Autorité Fédérale Belge en qualité d'autorité contractante pour le projet eID, en charge de la production, de la personnalisation, de l'initialisation et de la distribution des cartes pour étrangers. Les certificats sont insérés dans ces cartes par le CM, lequel génère également les paires de clés. En particulier, ses tâches sont limitées à celles mentionnées aux lots 1 et 3 du Cahier Spécial des Charges RRN 006/2001.

1.1.2 Relations entre les entités régies par ce CPS

La relation entre CERTIPOST en tant que CSP pour le " Foreigner CA " et les détenteurs de certificats, les étrangers, est dans une grande mesure régie par la loi du 19 juillet 1991 relative aux registres de population et aux cartes d'identité, telle que modifiée par la loi du 25 mars 2003, visée ci-après comme la "Loi sur les Cartes d'Identité" et la loi du 15 décembre 1980 concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers visée ci-après comme la "Loi sur les étrangers". CERTIPOST informe les détenteurs de certificats de leurs droits et obligations par le biais d'un prospectus au frais de l'Autorité Fédérale Belge et distribué par l'administration communale.

Les CA, RA et CM ont convenu que CERTIPOST assumerait le rôle de CSP et serait entièrement responsable envers le public.

Conformément à la norme ETSI 104.456 supportant la directive européenne (référence) en matière de signature électronique, Certipost assure la gestion de ses tâches CSP par le biais d'un PKI Management Board qui bénéficie de toute l'expérience requise.

À travers sa participation officielle aux réunions hebdomadaires sur l'état d'avancement du projet eID, auxquelles l'ensemble de parties susmentionnées sera dûment représenté, Certipost rassemble l'ensemble des informations nécessaires et pose toutes les questions pertinentes à ces parties pour assumer sa responsabilité de CSP. Les problèmes et les questions sont analysés au

[1] RRN est l'abréviation de "Rijksregister-Registre National". Le RRN est une administration public faisant partie du Service Public Fédéral Intérieur, responsable de la gestion entre autre du Registre National des personnes physiques [2] CM : abréviation de Card Manufacturer

sein du PKI Management Board. Si nécessaire, des propositions/corrections sont formulées lors de la réunion sur l'état d'avancement.

Le coordinateur du PKI management board, envers le eID CSP Steering dirigé par Fedict, fera part de tout problème ne pouvant être résolu par ce processus à l'échelon supérieur. Ce Steering est à même de faire appel à des experts externes pour obtenir un second avis et supporter la responsabilité en matière de règlement des litiges.

1.2 Portée du présent CPS

Un énoncé des pratiques de Certification (CPS) est une déclaration unilatérale des pratiques respectées par une autorité de certification lorsque celle-ci fournit des services de certification. Un CPS est une description exhaustive de la manière avec laquelle le CSP met ses services à disposition. Ce CPS ne devrait être utilisé que dans le domaine du CSP[2]. Le CPS vise à délimiter le domaine de prestation de services de certification aux étrangers et aux parties confiantes[3] dans le cadre du domaine du CSP. Ce CPS met également en exergue la relation entre le « Foreigner CA » et d'autres autorités de certification dans la hiérarchie PKI de l'Autorité Fédérale Belge comme la Belgium Root Certification Authority (BRCA)[4]. Il décrit également la relation entre le CSP et les autres organisations impliquées dans la fourniture des certificats pour les cartes pour étrangers (ci-après les " certificats pour étrangers").

Ce CPS fournit également des directives opérationnelles pour l'ensemble des étrangers et des parties confiantes, en ce compris les personnes physiques ou morales en Belgique et à l'étranger. Ce CPS fournit également les directives opérationnelles (PKI best practices) pour les autres autorités de certification, comme le BRCA, appartenant à la hiérarchie PKI de l'Autorité Fédérale Belge dans le cadre juridique des signatures électroniques et des cartes pour étrangers en Belgique. Qui plus est, ce CPS décrit les relations entre le CSP et l'ensemble des autres entités jouant un rôle dans le contexte de la carte pour étranger comme le Personnalisateur de la Carte ou l'Initialisateur. L'Autorité Fédérale Belge acquiert ces services par le biais du Contrat Cadre. Enfin, dans une perspective d'accréditation et de supervision, ce CPS fournit une guidance pour les autorités de supervision, les organes d'accréditation, les auditeurs accrédités etc. pour ce qui est des pratiques du CSP.

Ce CPS avalise et met en oeuvre les normes suivantes:

- RFC 2527: Internet X.509 Public Key Infrastructure – Politique de certificat et Pratiques de certification
- RFC 2459: Internet X.509 Public Key Infrastructure – Certificat et profil CRL.
- RFC 3039: Internet X.509 Public Key Infrastructure – Profil de certificat qualifié.
- RFC 2560: X.509 Internet Public Key Infrastructure – Protocole de validation de certificats en ligne - OCSP
- ETSI TS 101 456: Exigences politiques pour les autorités de certification délivrant des certificats qualifiés.
- ETSI TS 101 862: Profil de certificat qualifié.
- ETSI TS 102 042: Exigences politiques pour les autorités de certification délivrant des certificats de clés publiques (niveau normalisé uniquement).
- La norme ISO 1-7799 en matière de sécurité et d'infrastructure.

Le CPS aborde en détail les politiques et les pratiques techniques, procédurales et organisationnelles du CA pour ce qui est de l'ensemble des services de certification offerts et ce, durant la durée de vie complète des certificats délivrés par le "Foreigner CA". En même temps que

[2] Le domaine du CSP est la zone de compétence du CSP en matière de prestation de services de certification. En d'autres termes, le domaine du CSP n'englobe pas les applications utilisant les certificats, etc.

[3] Cf. paragraphe 1.7.7 (Parties confiantes: entités se fiant à un certificat)

[4] Le BRCA est le CA ayant certifié le "Foreigner CA". La confiance dans le BRCA implique automatiquement une confiance implicite dans le "Foreigner CA".

ce CPS, d'autres documents liés au processus de certification dans le contexte de la carte pour étranger peuvent avoir été pris en compte. Ces documents seront disponibles par le biais du répertoire du CSP à l'adresse: http://repository.eid.belgium.be.

Ce CPS est rendu disponible en ligne dans le répertoire du CSP à l'adresse http://repository.eid.belgium.be.

Le CSP accepte les commentaires relatifs à ce CPS adressés à: CSP pour le "Foreigner CA" p/a CERTIPOST, Centre Monnaie, 1000 Bruxelles.

Le présent CPS est conforme aux exigences formelles de l'Internet Engineering Task Force (IETF) RFC 2527, version 12 juillet 2001, sur le plan du format et du contenu. Alors que certains intitulés de sections sont inclus conformément à la structure du RFC 2527, le sujet peut ne pas s'appliquer nécessairement à la mise en œuvre des services de certification du CSP pour le "Foreigner CA". De telles sections sont indiquées au moyen de l'annotation "Section non applicable". Des changements éditoriaux mineurs aux prescriptions du RFC 2527 ont été insérés dans le présent CPS afin de mieux adapter la structure du RFC 2527 aux besoins de ce domaine d'application.

De plus amples informations liées à ce CPS et au CSP peuvent être obtenues auprès du CSP pour le "Foreigner CA" p/a CERTIPOST, Centre Monnaie, 1000 Bruxelles.

1.3 Les certificats sur la carte pour étranger

La loi belge du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité, telle que modifiée par la loi du 25 mars 2003, ci-après dénommée "la loi sur les cartes d'identité ", et les arrêtés royaux portant exécution de la loi, introduit la carte pour étranger. La carte pour étranger est une carte contenant des informations au format graphique imprimées sur la surface de la carte ainsi que des informations au format électronique dans une puce insérée dans la carte. La loi régit le cadre juridique pour la délivrance et l'utilisation de la carte pour étranger. Ce CPS aborde les aspects des pratiques de certification dans les limites de la législation belge. Dans l'exécution de son rôle en tant que CSP pour le "Foreigner CA", CERTIPOST est en premier lieu tenu de respecter les dispositions de la loi.

Pour permettre aux détenteurs d'une carte pour étranger de (i) s'identifier et (ii) de signer par voie électronique, les cartes contiennent, suivant leur âge, deux types de certificats numériques:

- Un certificat d'identité: le détenteur de la carte pour étranger peut utiliser ce certificat pour s'authentifier dans les transactions électroniques s'il avait atteint l'âge de 6 ans au moment de la demande de la carte. Le certificat d'identité contient l'identité du détenteur ainsi que la clé publique correspondant à la clé privée, stockée sur la carte pour les besoins de l'authentification d'un utilisateur. Cette clé privée peut être uniquement utilisée pour identifier un utilisateur de la carte pour étranger.
- Un Certificat Qualifié pour Signatures Electroniques (ou e-Signatures): ce certificat contient l'identité du détenteur et la clé publique correspondant à la clé privée, stockée sur la carte pour les besoins de la création d'une signature électronique uniquement. Ce certificat est appelé Certificat Qualifié conformément aux exigences de la directive européenne 99/93/CE. Le certificat qualifié pour signatures électroniques est conforme aux dispositions de la Loi sur la signature électronique et la Directive européenne 1999/93 et peut être activé dès que l'étranger a atteint l'âge de 18 ans.

Les exigences les plus pointues en matière de sécurité préconisent de ne pas utiliser les certificats d'identité pour des fins de signature électronique, mais d'utiliser à la place un certificat qualifié distinct pour la signature électronique. C'est la raison pour laquelle le Certificat d'Identité ne s'est pas vu octroyer le statut de certificat qualifié, permettant ainsi à toutes les parties concernées d'opérer une distinction très nette entre le certificat d'identité et le certificat qualifié pour signature Electronique.

L'activation des certificats sur la carte pour étranger est optionnelle. Dès lors, un étranger peut choisir d'"activer" ou non l'utilisation des clés et des certificats sur sa carte pour étranger. En activant les certificats sur sa carte pour étranger, l'étranger entre dans une relation contractuelle avec CERTIPOST dans son rôle de CSP pour le "Foreigner CA".

La technologie utilisée pour les services de certification pour ces certificats est la "technologie PKI". PKI (Public Key Infrastructure) est un acronyme pour un système de cryptographie de Clé Publique (Public Key) combiné à une infrastructure conçue pour fournir un niveau de sécurité pour

les informations électroniques communiquées et sauvegardées qui soit suffisant pour justifier la confiance en de telles informations par les entreprises, consommateurs, gouvernements et tribunaux.

L'organisme délivrant les certificats est appelé Autorité de Certification (CA, certification authority). L'organisme en charge de l'identification de la personne introduisant une demande de certificat est appelé quant à lui l'Autorité d'Enregistrement (RA, Registration Authority). Dans ce contexte, le rôle de l'émetteur des certificats est assumé par CERTIPOST. Le rôle de la RA est pris en charge par le RRN[5]. Toutefois, dans le contexte de la carte pour étranger, seule la RA est habilitée à inviter le "Foreigner CA" à délivrer un certificat à un étranger.

La RA ne procède pas à l'identification physique du demandeur même, mais délègue cette responsabilité aux Autorités d'Enregistrement Locales (LRA, Local Registration Authorities). Dans ce contexte, les administrations communales agiront en qualité de LRA. En tant que telles, les administrations communales feront office d'interface entre les demandeurs (en l'occurrence les étrangers) et la RA.

1.4 Relation entre ce CPS et d'autres documents

Comme décrit ci-dessus, le présent CPS est une déclaration unilatérale faite au public en général relative aux pratiques auxquelles le CSP pour le "Foreigner CA" se conforme lorsqu'il fournit des services de certification. Il s'agit d'une description exhaustive de la manière dont le CSP met ses services à disposition.

Conformément à la description plus détaillée reprise ci-après, le RRN, de concert avec les administrations communales, fait office de RA dans le domaine du CSP, à l'exclusion de tout autre. Seuls le RRN et les administrations communales peuvent décider de la délivrance d'un certificat en vertu du présent CPS. Le RRN peut néanmoins désigner une ou plusieurs parties tierces pour mener à bien les tâches de RA à l'intérieur du domaine du CSP.

Seuls le RRN, les administrations communales ou le CSP peuvent décider de la suspension et de la révocation d'un certificat en vertu du présent CPS.

La relation entre l'Etat belge et le CSP pour le "Foreigner CA" est régie dans un accord cadre. En cas de contradiction entre ce CPS et l'accord cadre, priorité devrait être donnée aux dispositions de l'accord cadre. Ce CPS ne crée aucun droit ni obligation additionnels pour l'Etat belge, CERTIPOST, ZETES ni toute autre partie impliquée dans l'assurance et la gestion de la carte pour étranger. Le CPS a pour objectif premier de préciser les dispositions légales et contractuelles et d'informer l'ensemble des parties intéressées des pratiques du CSP pour le "Foreigner CA".

1.5 Positionnement du "Foreigner CA" dans la hiérarchie CA

Pour utiliser pleinement la carte pour étranger, il convient de s'assurer tant de l'identité de l'étranger que de l'identité de l'infrastructure technique, en clair les serveurs requis dans les applications de l'Etat belge. Voilà pourquoi il convient d'utiliser différents types de certificats audelà des certificats pour étrangers. Le "Foreigner CA" appartient à un domaine plus large des autorités de certification de l' Autorité Fédérale Belge. Pour faciliter l'instauration d'un climat de confiance entre les différentes Autorités de Certification participantes, l'Autorité Fédérale Belge a mis sur pied une hiérarchie PKI.

Au sommet de cette hiérarchie, trône le "Belgium Root CA (BRCA)" dont le but, entre autres choses, est d'instaurer la confiance entre les différentes autorités de certification à l'intérieur du domaine de l'Autorité Fédérale Belge. Le BRCA (auto-signé) a certifié chacune des clés privées des autorités de certification dans le domaine de l'Autorité Fédérale Belge, en ce compris le "Foreigner CA". En validant le certificat d'un tel CA, la confiance dans le BRCA peut également être appliquée

[5] RRN est l'acronyme de "Rijksregister-Registre National". Le RRN est une administration au sein du Service Public Fédéral Intérieurs. Il est par exemple en charge de la gestion du Registre National des personnes physiques.

au CA qu'il a certifié. Dans la mesure où le BRCA bénéficie de la confiance, l'on peut également faire confiance au certificat de l'utilisateur final.

La confiance dans le BRCA à l'intérieur des applications logicielles est également établie par le biais d'un "root sign" réalisé par un prestataire tiers (digicert cybertrust global), dont la racine a été largement intégrée dans le logiciel d'application.

Le BRCA opère suivant des pratiques publiées dans un CPS dédié disponible sur http://repository.eid.belgium.be.

La confiance dans les certificats pour étranger peut être vérifiée comme suit:

1. Création d'un chemin sécurisé.

   Le Certificat pour étranger est contrôlé pour vérifier qu'il a bel et bien été délivré par le "Foreigner CA". Conformément à cela, le certificat du "Foreigner CA" est contrôlé dans le but de s'assurer qu'il a bien été émis par le BRCA. Lorsque le résultat de ces contrôles s'avère positif, la confiance accordée au BRCA peut être répercutée via le "Foreigner CA" sur le certificat personnalisé pour étranger.

   Vérification du certificat BRCA.

   D'une manière générale, le certificat BRCA est mentionné dans la mémoire des certificats de l'application en tant que certificat de confiance. Dans l'éventualité improbable où l'utilisateur final serait averti du fait que le certificat BRCA ne serait plus valable, il lui suffit de supprimer le certificat BRCA de la mémoire des certificats pour exclure ce domaine de ses domaines de confiance pour s'assurer que cette partie de la vérification a échoué.

2. La vérification du certificat "Foreigner CA" peut être effectuée en prenant les mesures suivantes:

   2.1. Contrôle de la validité du certificat "Foreigner CA" (ex. vérification de la période de validité)

   2.2. Contrôle de l'état du certificat "Foreigner CA" (ex. vérification de la suspension ou de la révocation).[6]

3. La vérification du Certificat peut être effectuée en prenant les mesures suivantes:

   3.1. Contrôle de la validité du Certificat (ex. vérification de la période de validité).

   3.2. Contrôle de l'état du Certificat (ex. vérification de la suspension ou de la révocation).

D'une manière générale, la majeure partie pour ne pas dire l'ensemble de ces opérations sont réalisées de manière automatique par l'application utilisant les certificats, de sorte que l'interaction avec l'utilisateur final est minime voire totalement absente.

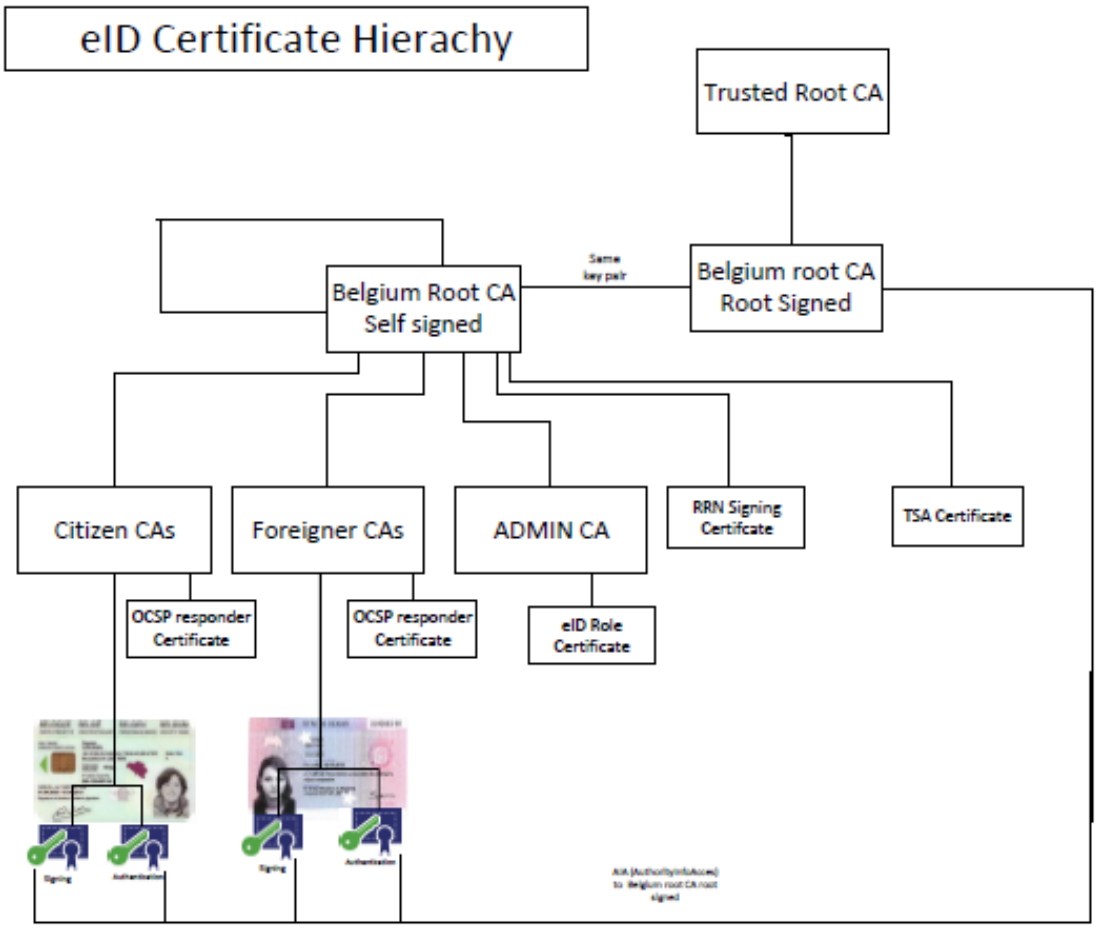
La hiérarchie de confiance des certificats pour étrangers suit l'architecture ci-dessous:

1. Une petite hiérarchie pour laquelle l'ensemble des informations requises pour valider les certificats hors ligne peut être sauvegardées sur la carte.

2. Une préférence marquée pour la confiance automatisée dans les certificats délivrés par l'infrastructure de l'État belge, sans nécessiter d'intervention dans le chef de l'utilisateur final, pour la vérification en ligne.

Cette hiérarchie plus complexe est décrite au schéma 1 ci-dessous:

[6] Les services de vérification du statut fournis par le CA sont décrits au chapitre 4.10 Services d'état du certificat en page 22.



Pour répondre à ces deux exigences, la hiérarchie PKI consiste en une combinaison d'un modèle à deux couches et d'un modèle à trois couches.

Dans le modèle à deux couches, le "Foreigner CA" et le Belgium Root CA[7] auto-signé forment une hiérarchie, laquelle, en mode hors ligne, permet la validation de la signature et des certificats d'authentification. Dans ce modèle, la clé du Belgium Root CA est auto signée. Dans un tel cas, la partie effectuant la validation (ex. l'officier des douanes, l'officier de police etc.) peut utiliser le certificat BRCA auto signé provenant de sa propre carte d'identité électronique et l'utiliser pour valider le certificat "Foreigner CA" et les certificats de la carte pour étranger à valider.

Dans le modèle à trois couches, le "Foreigner CA", le Belgium Root CA signé à la racine et le digicert cybertrust global Root CA forment une hiérarchie. Dans ce modèle, la même clé privée utilisée pour le Belgium Root CA auto signé est cette fois certifiée par le digicert cybertrust global Root CA. Cette approche permet la validation automatique dans les applications les plus couramment utilisées, comme les navigateurs par exemple, car ceux-ci ont déjà intégré le certificat digicert cybertrust globalTop Root CA et ils le reprennent comme un certificat de confiance. Tout comme le "Foreigner CA " hérite de la confiance du BRCA, le BRCA hérite de la

[7] Un certificat auto-signé est un certificat signé avec la clé privée de l'entité certifiée elle-même. Etant donné qu'il n'y a pas de point de confiance plus élevé dans la hiérarchie de confiance, aucune confiance ne peut être instaurée sur ce certificat ou sur tout certificat qui occupe une position inférieure dans la hiérarchie si ce certificat auto-signé n'est pas fiable. Ceci est toutefois un cas qui doit se produire très rarement.

confiance du digicert cybertrust global Root CA. Ce modèle à trois couches rend donc superflue l'importation individuelle du certificat auto signé Belgium Root CA.

Comme tant le Belgium Root CA auto-signé que le Top Root CA signé à la racine belge partagent la même paire de clés utilisant tous deux certificats distincts, un certificat signé par la clé privée de cette paire de clés peut être validé avec les deux certificats Belgium Root.

Dans la plupart des cas, le développeur de l'application aura prévu l'un des deux modèles à utiliser et l'utilisateur final n'aura pas à choisir entre les deux modèles.

1.6 Nom et identification du document

Le présent CPS peut aussi être identifié par n'importe quelle partie via les OID suivants[8] :

- l'OID 2.16.56.1.1.1.7.1. pour le certificat de signature électronique,
- l'OID 2.16.56.1.1.1.7.2 pour le certificat d'identité.

1.7 Participants PKI

Plusieurs parties forment les participants de cette hiérarchie PKI. Les parties citées ci-après, y compris toutes les autorités de certification, la RA, les LRA (les administrations communales), les étrangers et les parties confiantes sont collectivement appelés les participants PKI.

1.7.1 Autorité de certification pour le Foreigner CA

Une autorité de certification (CA) est un organisme qui émet des certificats numériques utilisés dans le domaine public, dans un contexte commercial ou dans le cadre de transactions. Le "Foreigner CA" est une telle autorité de certification.

Le CA bénéficie d'une autorisation de délivrance de certificats pour étrangers. Cette autorisation est accordée par la Belgium Root Certification Authority (ci-après dénommée "BRCA").

Le CA garantit la disponibilité de tous les services relatifs aux certificats, y compris la délivrance, la révocation, la vérification d'état et l'horodatage, dès qu'ils deviennent disponibles ou nécessaires dans des applications spécifiques.

Le CA est supervisé conformément aux dispositions de l'article 20 de la loi sur les signatures électroniques.

Le CA est établi en Belgique. Il peut être contacté à l'adresse publiée par ailleurs dans le présent CPS. En vue de la fourniture de services CA, comprenant la délivrance, la suspension, la révocation, le renouvellement, la vérification d'état de certificats, le CSP exploite un système sécurisé et prévoit un centre de secours en Belgique pour assurer la continuité des services CA.

Le domaine de responsabilité du CA couvre la gestion globale du cycle de vie d'un certificat, notamment :

- la délivrance ;
- la suspension/réhabilitation après suspension ;
- la révocation ;
- la vérification d'état (service d'état du certificat) ;
- le service de répertoire.

1.7.2 Fournisseur de Root Sign

[8] Object IDentifier = Identificateur d'objet.

Le fournisseur de "root sign" garantit la confiance en la BRCA dans des applications très répandues. Le fournisseur de root sign veille à ce que ces applications maintiennent leur confiance dans sa racine et notifie à la RA tous les événements affectant la confiance dans sa propre racine. Le fournisseur de root sign de la BRCA est digicert cybertrust global (http://cybertrust.omniroot.com/repository/).

1.7.3 Autorité d'enregistrement et autorités d'enregistrement locales

Le RRN (Registre National) et les administrations communales sont la RA à l'intérieur du domaine de CSP pour le "Foreigner CA", à l'exclusion de tout autre organisme. Le RRN est constitué et agit en vertu des dispositions de la Loi sur le Registre National et de la Loi sur les cartes d'identité.

Seuls le RRN et les administrations communales peuvent décider de la délivrance d'un certificat au sens du présent CPS. Le RRN peut désigner une tierce partie en vue de prendre en charge des tâches de la RA à l'intérieur du domaine de "Foreigner CA".

Seuls le RRN, les administrations communales ou le CSP peuvent décider de la suspension et de la révocation d'un certificat au sens du présent CPS.

Le RRN (registre national) et les administrations communales sont la RA à l'intérieur du domaine de CSP pour le "Foreigner CA", à l'exclusion de tout autre organisme. Les LRA enregistrent et vérifient les données de l' étranger pour le compte de la RA. En ce qui concerne l'enregistrement, les LRA n'ont aucun contact direct avec le "Foreigner CA".

La RA présente au "Foreigner CA" les données nécessaires en vue de la génération et de la révocation des certificats.

Les LRA (les administrations communales) collaborent directement avec les étrangers en vue de proposer des services de certification publics à l'utilisateur final. Plus spécifiquement, les LRA :

- envoient ci nécessaire à l'étranger la lettre de convocation l'invitant au besoin à contacter le service administratif approprié, par exemple quand la carte pour étranger doit être renouvelée ;
- suivent toutes les procédures requises en vue de compléter le document de base[9]. Par la suite, l'étranger approuve le document source. La LRA envoie ensuite les données sécurisées du document source au personnalisateur de cartes afin de poursuivre le traitement de la demande de certificat. Le personnalisateur de cartes ne délivre une carte pour étranger qu'après une approbation de la RA résultant d'une demande du personnalisateur de cartes ;
- lancent via la RA la procédure de demande de changement de statut d'un certificat vers le CA ;
- remettent à l' étranger les cartes électroniques émises.

La RA collabore indirectement avec les étrangers et directement avec le CA en vue de proposer des services de certification publics à l'utilisateur final. Plus spécifiquement, la RA :

- met en place un service d'assistance où le titulaire de la carte pour étranger peut notifier la perte, le vol ou la destruction de sa carte pour étranger quand il ne peut pas accomplir cette formalité auprès de l'administration communale ou des services de police. Ce service d'assistance est dénommé “RA Helpdesk” ci-après ;
- procède à l'enregistrement des étrangers pour des services de certification ;
- invite le CA à délivrer un certificat quand une demande est approuvée ;
- lance la procédure de révocation d'un certificat et demande au CA de révoquer ou de suspendre un certificat.

La RA présente au "Foreigner CA" les données nécessaires à l'élaboration des certificats. Pour chaque certificat, la RA fournit l'identité du titulaire et le numéro de série du certificat requis ainsi que la clé publique associée à l' étranger à mentionner dans ledit certificat.

Toutes les communications entre la LRA, la RA et le CA concernant l'une des phases du cycle de vie de certificats sont sécurisées par des techniques de chiffrement et de signature fondées sur un

[9] Le document de base sert à collecter des informations permettant de délivrer une carte d'identité. Le Service Public Fédéral Intérieur transmet le modèle de ce document aux administrations communales.

système cryptographique à clé publique en vue de garantir la confidentialité et l'authentification mutuelle. Il s'agit des échanges d'informations concernant la demande, la délivrance, la suspension, la réhabilitation après suspension et la révocation de certificats.

1.7.4 Personnalisateur de cartes

Le personnalisateur de cartes transforme des cartes intelligentes non personnalisées en cartes pour étrangers personnalisées en imprimant les données d'identité et la photographie de l'étranger sur la carte. Le personnalisateur de cartes est également responsable de la transmission sécurisée de ces cartes personnalisées à l'initialisateur de cartes. Le rôle de personnalisateur de cartes est actuellement rempli par la S.A. ZETES [10] en vertu d'un accord-cadre conclu avec l'Autorité Fédérale Belge.

1.7.5 Initialisateur de cartes

L'initialisateur de cartes fournit les services suivants :

- génération des paires de clés requises pour la carte ;
- stockage des deux certificats sur la carte ;
- génération des codes d'activation personnels du demandeur et de l'administration communale et du code PIN initial du demandeur ;
- chargement des certificats root gouvernementaux actifs sur la carte ;
- fourniture de la carte pour étranger à l'administration communale ; • fourniture du code d'activation personnel et du code PIN au demandeur ;
- enregistrement des données dans le registre des étrangers.

Le rôle de l'initialisateur de cartes est actuellement rempli par la S.A. ZETES en vertu d'un accordcadre conclu avec l'Autorité Fédérale Belge.

1.7.6 Usagers

Les usagers des services CA dans le domaine "Foreigner CA" sont des étrangers titulaires d'une carte pour étranger avec certificats activés conformément à la loi sur les cartes d'identité et la loi sur les étrangers. Dans la suite du présent document, le terme "usager" peut être remplacé par le terme "étranger".

Ces étrangers :

- sont identifiés dans les deux certificats;
- détiennent les clés privées correspondant aux clés publiques consignées dans leurs certificats respectifs.

Les étrangers ont le droit de signaler au début du processus de demande de carte pour étranger s'ils souhaitent des certificats. La carte pour étranger est délivrée aux étrangers dont les certificats sont chargés. Pour les étrangers non désireux d'utiliser les certificats, ces certificats seront révoqués. Pour les étrangers qui n'ont pas encore atteint l'âge de 6 ans au moment de la demande d'une carte pour étranger, les certificats d'identification et de signature électronique sont automatiquement révoqués.

Pour les étrangers n'ayant pas encore atteint l'âge de 18 ans, le certificat de signature électronique est automatiquement révoqué à la demande d'une carte pour étranger.

[10] http://www.zetes.com

1.7.7 Parties confiantes

Les parties confiantes sont des entités, parmi lesquelles figurent les personnes physiques et morales, qui s'appuient sur un certificat et/ou une signature numérique vérifiable par référence à une clé publique énoncée dans un certificat pour étranger.

Pour vérifier la validité d'un certificat numérique qu'elles reçoivent, les parties confiantes doivent toujours opérer une vérification en se basant sur la période de validité du certificat et sur la déclaration de validité du certificat auprès du service de vérification de CA (p. ex. OCSP, CRL, Delta CRL ou interface Web) avant de s'appuyer sur des informations figurant dans un certificat.

1.8 Utilisation du certificat

L'utilisation des certificats sur la carte pour étranger fait l'objet de certaines restrictions.

Les certificats d'identification délivrés par le "Foreigner CA" peuvent être employés pour des transactions d'authentification électroniques spécifiques supportant un accès à des sites Web et à d'autres contenus en ligne, au courrier électronique, etc., au moment de leur mise à disposition par l'Autorité Fédérale Belge. Les prescriptions actuelles en matière de sécurité recommandent de ne pas employer des certificats d'identité à des fins de signature électronique. Le CSP pour le "Foreigner CA" décline dès lors toute responsabilité vis-à-vis des parties confiantes dans tous les cas où le certificat d'identité est utilisé pour la génération de signatures électroniques.

1.9 Gestion administrative

La gestion administrative est réservée au CSP pour le "Foreigner CA", p/a CERTIPOST, Centre Monnaie, 1000 Bruxelles.

1.10 Définitions et acronymes

Des listes des définitions et acronymes figurent à la fin du présent CPS.

2. Responsabilités en matière de publication et d'archivage

Le CSP publie les informations relatives aux certificats numériques qu'il délivre dans un ou des référentiels en ligne accessibles au public dans le domaine Internet belgium.be. Le CA se réserve le droit de publier des informations concernant l'état du certificat dans des répertoires de tiers.

Le CSP conserve un répertoire en ligne des documents dans lequel il révèle certaines de ses pratiques et procédures ainsi que le contenu de certaines de ses politiques, y compris son CPS, qui sont accessibles sous http://repository.eid.belgium.be. Le CA se réserve le droit de mettre à disposition et de publier des informations sur ses politiques par tous les moyens qu'il juge appropriés.

Les participants PKI sont avertis que le CA peut publier des informations qu'ils soumettent directement ou indirectement au CA sur des répertoires publics, à des fins associées à la fourniture d'informations sur l'état des certificats électroniques. Aux intervalles de temps dont la fréquence est indiquée dans le présent CPS, le CA publie des informations sur l'état des certificats numériques.

Le CA crée et tient à jour un répertoire de tous les certificats qu'il a délivrés. Ce répertoire signale aussi l'état d'un certificat délivré.

Le CA publie des CRL [11] à intervalles réguliers sur http://crl.eid.belgium.be. Le CA publie régulièrement des "Delta CRL" contenant les modifications apportées depuis la publication de la CRL ou Delta CRL précédente. Chaque nouvelle CRL publiée contient toutes les mises à jour des Delta CRL antérieures.

Le CA met à disposition un serveur OCSP [12] à l'adresse http://ocsp.eid.belgium.be en vue d'informer sur l'état d'un certificat délivré par le CA à la demande d'une partie confiante, conformément à IETF RFC 2560. Le statut d'un certificat peut aussi être vérifié à l'adresse Internet suivante: http://status.eid.belgium.be. L'état d'un certificat figurant dans une CRL ou une Delta CRL doit correspondre aux informations fournies par le serveur OCSP.

Le CA tient à jour le point de diffusion de la CRL et les informations disponibles à cet URL jusqu'à la date d'expiration de tous les certificats contenant le point de diffusion de la CRL. Des versions approuvées des documents à publier sur le répertoire sont téléchargées vers le serveur dans les 24 heures.

Vu leur caractère sensible, le CA ne publie pas certains sous composants et éléments de ces documents, notamment certains contrôles de sécurité, des procédures liées entre autres au fonctionnement d'autorités d'enregistrement, des stratégies de sécurité internes, etc. L'accès conditionnel à ces documents et pratiques documentées est néanmoins accordé, pour vérification, à des parties désignées envers lesquelles le CA est tenu d'un devoir.

2.1 Contrôle d'accès aux répertoires

Bien que le CSP mette tout en œuvre pour maintenir la gratuité de l'accès à son répertoire public, il pourrait faire payer, dans le cadre de son contrat avec le gouvernement, des services tels que la publication d'informations d'état dans des bases de données tierces, des répertoires privés, etc.

Le service OCSP, le service de vérification du statut des certificats par interface Web, le référentiel de certificats, les CRL et les Delta CRL sont mis à la disposition du public sur le site Internet du CA et sont accessibles via les réseaux du l'Autorité Fédérale Belge.

Dans le cadre du contrat conclu avec l'Autorité Fédérale Belge, les restrictions d'accès à des services fournis par le CSP incluent :

par l'entremise de l'interface publique au répertoire de certificats, un seul certificat peut être délivré pour chaque demande formulée par toute partie à l'exception de la RA ;

le CA peut prendre des mesures raisonnables en vue d'assurer une protection contre les abus du service OCSP, du service de vérification d'état par interface Web et du service de téléchargement des CRL et des Delta CRL. En particulier : le CA peut restreindre à 10 demandes par jour la fréquence de traitement des demandes OCSP formulées par un seul utilisateur si le CA peut démontrer un quelconque abus du système de la part de l'utilisateur. Le CA ne devrait pas restreindre le traitement de demandes OCSP pour une partie qui, de par la nature de ses activités, requiert une vérification fréquente d'état OCSP ;

le CA peut restreindre à 10 demandes par jour la fréquence de traitement de demandes de vérification d'état de certificats par interface Web qui sont formulées par un seul utilisateur .

[11] Une CRL ou liste de révocation de certificats (Certificate Revocation List) est une liste qui a été émise et signée numériquement par un CA et qui reprend les numéros de séries des certificats révoqués et suspendus. Cette liste doit être consultée systématiquement par les parties confiantes avant de s'appuyer sur des informations figurant dans un certificat.

[12] Le protocole d'état de certificat en ligne (RFC 2560) est une ressource d'informations d'état en temps réel qui sert à déterminer l'état actuel d'un certificat numérique sans devoir recourir à des CRL.

3. Identification et authentification

3.1 Dénomination

Les règles de dénomination et d'identification des étrangers pour les besoins des certificats sont les mêmes que les règles légales appliquées à la dénomination et à l'identification des étrangers pour les cartes pour étrangers.

3.2 Validation de l'identité initiale

L'identification de l'étranger qui demande une carte pour étranger reposera sur les procédures et règles applicables à la délivrance de cartes pour étranger. La RA définit les procédures à mettre en œuvre par les LRA.

3.3 Identification et authentification pour des demandes de recomposition (re-key)

L'identification et l'authentification du étranger qui demande la recomposition est soumise à l'application des procédures spécifiées par le RA et mis en œuvre par le LRA.

3.4 Identification et authentification pour des demandes de révocation et de suspension

L'identification de l' étranger qui demande une révocation ou une suspension de ses certificats sur les procédures et règles applicables à la délivrance de cartes pour étrangers.

L'identification et l'authentification de titulaires demandant la révocation ou la suspension de leurs certificats seront exécutées par l'entité qui reçoit la demande. Il peut s'agir :

- de l'administration communale,
- des services de police,
- du RA Helpdesk constitué à cette fin par la RA.

Par la suite, cette entité transmet aussitôt toutes les demandes de révocation au CA par l'entremise de la RA. La RA représente le seul point de contact du CA pour les demandes de révocation.

4. Exigences opérationnelles posées au cycle de vie d'un certificat

Toutes les entités du domaine du CSP, y compris les LRA, les étrangers, les parties confiantes et/ou les autres participants, sont constamment tenus d'informer directement ou indirectement la RA de toutes les modifications touchant aux informations contenues dans un certificat durant la période opérationnelle dudit certificat ou de tout autre fait affectant concrètement la validité d'un certificat. La RA prend alors les mesures qui s'imposent afin de rétablir la situation (p. ex. demander au CA de révoquer les certificats existants et de générer de nouveaux certificats avec les données correctes).

Le CA ne délivre, révoque ou suspend des certificats qu'à la demande de la RA, à l'exclusion de toute autre autorité, sauf sur instruction explicite de la RA.

Dans l'exécution de ses tâches, le CSP fait appel aux services d'agents tiers. Le CSP assume, à l'égard des étrangers et des parties confiantes, la pleine responsabilité des actes ou omissions de tout agent tiers auquel il fait appel pour la fourniture de services de certification.

4.1 Demande de certificat

Le processus d'inscription de l'étranger demandeur des certificats fait partie intégrante du processus de traitement de la carte pour étranger par son administration communale, c'est-à-dire la LRA. La LRA met en œuvre les procédures d'inscription des étrangers prévue par la RA.

4.2 Traitement de la demande de certificat

La LRA donne suite à une demande de certificat pour valider l'identité du demandeur conformément à la procédure relative à la demande de carte pour étranger. Les procédures de validation de l'identité d'un demandeur font l'objet d'un document spécifique.

Dans la foulée d'une demande de certificat, la LRA approuve ou rejette la demande de carte pour étranger comprenant aussi la demande de certificat. Si la demande est approuvée, la LRA transmet les données d'enregistrement à la RA. À son tour, la RA approuve ou rejette la demande.

4.3 Délivrance du certificat

Une fois la demande de certificat approuvée, la RA envoie une demande de délivrance de certificat au CA. Le CA ne vérifie pas la complétude, l'intégrité et l'unicité des données soumises par la RA, mais se fie totalement à la RA pour ce qui est de l'exactitude de toutes les données. Le CA se borne à contrôler que le numéro de série de certificat affecté à la demande par la RA est en fait un numéro de série unique qui n'a pas encore été attribué à un autre certificat, auquel cas il le notifie à la RA.

Toutes les demandes émanant de la RA sont approuvées dans la mesure où :

- elles sont formatées valablement,
- elles transitent par le canal de communication sécurisé adéquat,
- elles ont subi toutes les vérifications qui s'imposent conformément au contrat du CA.

Le CA vérifie l'identité de la RA en se fondant sur le justificatif d'identité présenté.

Le CA s'assure que le certificat délivré contient toutes les données qui lui ont été présentées dans la demande de la RA et, en particulier, un numéro de série affecté au certificat par la RA. Après la délivrance, le CA publie un certificat délivré sur un répertoire.

Après la délivrance, le CA suspend le certificat. Le certificat est ensuite transmis à la RA.

La RA prie l'initialisateur de cartes de charger les certificats sur la carte pour étranger. L'initialisateur de cartes transmet par un moyen sécurisé la carte pour étranger avec les certificats à la LRA.

4.4 Acceptation du certificat

En présence de l'étranger, la LRA active la carte pour étranger qui reste à l'état "suspendu" jusqu'à ce stade. L'étranger et la LRA ont tous deux besoin des données d'activation de la carte qui doit être fournie par l'initialisateur de cartes par un moyen sécurisé. La carte ne peut être activée qu'au moyen des données d'activation combinées de la LRA et de l' étranger.

Il incombe uniquement à l'étranger (en cas de demande d'une carte pour étranger à partir de 12 ans) ou à la personne / aux personnes chargée(s) d'exercer l'autorité parentale pour un enfant de moins de 12 ans (en cas de demande d'une carte pour étranger jusqu'à 12 ans) de décider s'il/elle(s) souhaite(nt) activer ou non les certificats. Un défaut d'activation des certificats par l'étranger peut restreindre l'accès à certains services proposés par l'État belge ainsi que par d'autres fournisseurs tiers sur la base de l'infrastructure eID existant en Belgique et à l'étranger.

Le processus d'activation impose d'envoyer, via la RA, une demande de réhabilitation après suspension au CA. Une fois les certificats activés, l'étranger doit tester les certificats et valider leurs contenus. Si la validation réussit, le certificat est réputé accepté.

Un certificat peut être rejeté, par exemple si les données relatives à l' étranger sont inexactes ou si l'étranger n'a pas atteint l'âge légal pour l'utilisation du certificat.

Des objections à l'acceptation d'un certificat délivré sont notifiées à la RA via la LRA en vue de prier le CA de révoquer les certificats et d'émettre ultérieurement un nouveau certificat avec les données correctes.

4.5 Paire de clés et emploi du certificat

L'emploi des clés et des certificats implique les responsabilités exposées ci-après.

4.5.1 Droits et obligations de l' étranger

Sauf indication contraire dans le présent CPS, les droits et obligations de l'étranger sont les suivants :

- ne pas manipuler un certificat ;
- employer les certificats aux seules fins légales et autorisées dans le respect du CPS ;
- utiliser un certificat dans la mesure du raisonnable compte tenu des circonstances ;
- éviter la compromission, la perte, la divulgation, la modification ou tout autre emploi non autorisé de ses clés privées.

4.5.2 Droits et obligations de la partie confiante

Une partie s'appuyant sur un certificat CA :

- validera un certificat à l'aide d'une CRL, d'une Delta CRL, d'un OCSP ou d'une procédure de validation de certificat Internet, conformément à la procédure de validation du chemin du certificat ;
- fera confiance à un certificat seulement s'il n'a pas été suspendu ou révoqué ;
- s'appuiera sur un certificat dans la mesure du raisonnable compte tenu des circonstances.

4.6 Renouvellement du certificat

Les certificats de l'étranger seront renouvelés

- en cas de renouvellement de la carte pour étranger,
- lorsque l'étranger demande la recomposition après la révocation des certificats.

4.7 Recomposition (re-key)

Après révocation les certificats ne peuvent plus être activés et doivent dès lors être remplacés par de nouveaux. Sur demande de l'étranger, le LRA générera une nouvelle paire de clés sur la carte pour étranger pour ensuite remplacer les certificats révoqués par les nouveaux.

4.8 Modification du certificat Section sans objet.

4.9 Révocation et suspension du certificat

Jusqu'à leur acceptation par l'étranger, les certificats demeurent suspendus dans une carte pour étranger. L'activation initiale d'un certificat doit avoir lieu dans le mois suivant son émission. La RA et les LRA font diligence pour se conformer à cette exigence.

Pour demander la suspension ou la révocation d'un certificat, un étranger doit contacter une LRA, les services de police ou le RA Helpdesk. Alors que les heures d'ouvertures d'une LRA sont limitées, le RA Helpdesk est accessible 24 heures sur 24, 7 jours sur 7.

Les services de police, la LRA ou le RA Helpdesk font diligence pour demander la suspension des certificats via la RA :

- après une notification, par l'étranger, de l'existence de soupçons concernant une perte, un vol, une modification, une divulgation non autorisée ou toute autre compromission de la clé privée de l'un et/ou l'autre de ses deux certificats;
- si l'exécution d'une obligation de la RA au sens du présent CPS est retardée ou empêchée par une catastrophe naturelle, une panne informatique, une interruption des télécommunications ou toute autre cause indépendante de la volonté raisonnable de la personne et crée en conséquence un doute quant à la menace ou à la compromission matérielle des informations d'une tierce personne ;
- après une notification, par l'étranger, de l'existence d'une perte, d'un vol, d'une modification, d'une divulgation non autorisée ou de toute autre compromission de la clé privée de l'un et/ou l'autre de ses deux certificats.
- Les informations contenues dans un certificat ont été modifiées.
- L'exécution d'une obligation de la RA au sens du présent CPS est retardée ou empêchée par une catastrophe naturelle, une panne informatique, une interruption des télécommunications ou toute autre cause indépendante de la volonté raisonnable de la personne et crée en conséquence une menace ou une compromission matérielle pour les informations d'une tierce personne.

À la demande de la RA, le CA suspend ou révoque les certificats.

La RA révoque un certificat suspendu après une période d'une semaine si elle ne reçoit pas de l'étranger une notification de réhabilitation du certificat.

Dans des circonstances spécifiques (p. ex. une catastrophe a été évitée, une clé CA se caractérise par une violation de sécurité, etc.), le CSP peut demander la suspension et/ou la révocation de certificats. Le CSP demande au eID CSP steering l'autorisation de procéder à ces révocations. Selon le degré d'urgence, il peut toutefois arriver que le eID CSP Steering ne soit averti qu'une fois le processus terminé. La RA veille à prévenir les étrangers concernés de cette suspension/révocation.

Les parties confiantes doivent utiliser les ressources en ligne que le CA met à leur disposition via son référentiel afin de vérifier l'état des certificats avant de s'appuyer sur eux. Le CA met à jour en conséquence l'OCSP, le service de vérification d'état de la certification par interface Web, les CRL et les Delta CRL. Les CRL sont actualisées fréquemment, au minimum toutes les trois heures. Le CA donne accès aux ressources OCSP et à un site Web sur lequel les requêtes d'état peuvent être soumises.

4.9.1 Durée et fin de la suspension et de la révocation

Une suspension peut durer sept jours civils maximum pour permettre d'établir les conditions qui ont motivé la demande de suspension. Si ces conditions ne peuvent pas être démontrées, un étranger peut demander la réactivation (réhabilitation après suspension) des certificats aux conditions suivantes :

- l'étranger a établi sans la moindre équivoque que ses soupçons concernant une perte, un vol, une modification, une divulgation non autorisée ou toute autre compromission de la clé privée de l'un et/ou l'autre de ses deux certificats n'étaient pas fondés ;

- il n'y a aucune autre raison de douter de la fiabilité et de la confidentialité des clés privées de ses deux certificats.

Pour demander la réhabilitation après suspension de ses certificats, un étranger doit contacter son/sa LRA (son/sa commune de résidence)

.

La LRA font diligence pour demander la réhabilitation après suspension d'une paire de certificats via la RA :

- après avoir été notifiés par l'étranger que les soupçons concernant une perte, un vol, une modification, une divulgation non autorisée ou toute autre compromission de la clé privée de l'un et/ou l'autre de ses deux certificats n'étaient pas fondés ;
- si les soupçons ont incontestablement montré que les informations d'une tierce personne ne seraient pas menacées ou compromises matériellement par le retard ou l'empêchement de l'exécution d'une obligation de la RA au sens du présent CPS du fait d'une catastrophe naturelle, d'une panne informatique, d'une interruption des télécommunications ou de toute autre cause indépendante de la volonté raisonnable de la personne ;
- à la demande de la RA, le CA suspend ou révoque une paire de certificats.

Le CA révoque automatiquement un certificat suspendu après une période d'une semaine si, dans l'intervalle, il ne reçoit pas de la RA une notification de réhabilitation du certificat. Le CA notifie toutes les révocations effectuées à la RA.

Le CA publie des avis concernant les certificats suspendus ou révoqués dans le référentiel.

4.10 Services d'état du certificat

Le CA met à disposition des services de vérification d'état des certificats, parmi lesquels des CRL, des Delta CRL, des OCSP et des interfaces Web adéquates.

CRL et delta CRL http://crl.eid.belgium.be

Une Delta CRL reprend tous les ajouts depuis la publication de la dernière CRL de base.

Les CRL et les Delta CRL sont signées et datées par le CA.

Une CRL est publiée toutes les 24 heures, à une heure convenue. Une Delta CRL est publiée toutes les 3 heures, selon un horaire convenu.

Le CA met à disposition sur son site Web toutes les CRL et Delta CRL publiées au cours des 12 mois précédents.

OCSP http://ocsp.eid.belgium.be

Le CA met les réponses OCSP à la disposition de l'administration belge qui les exploite via ses propres réseaux de l'administration publique.

Le service OCSP de CSP est cascadé avec le service OCSP de la BRCA.

Interface Web du service de vérification d'état http://status.eid.belgium.be

Une interface Web simple donne accès aux services de vérification d'état et permet à un utilisateur d'obtenir des informations sur l'état d'un certificat. Le CA met ces interfaces Web d'accès aux services de vérification d'état à la disposition de l'administration belge qui les exploite via ses propres réseaux de l'administration publique et dans le cadre de ceux-ci.

Pour chaque mois civil, le temps total d'indisponibilité de chacun des services CA suivants, mesuré en minutes cumulées sur le mois complet, ne doit pas excéder 0,5 % du nombre total de minutes du mois civil concerné :

- vérification OCSP d'état du certificat à la suite d'une demande introduite par le RRN, un usager ou une partie confiante ;
- téléchargement de CRL ou de delta CRL via Internet ou les réseaux publics ;

- service de vérification d'état de certificats par interface Web.

L'indisponibilité du service OCSP, du service de téléchargement de CRL et de delta CRL et du service de vérification d'état par interface Web comprend l'indisponibilité de l'infrastructure locale du CA, notamment les serveurs, réseaux et coupe-feux locaux, mais n'inclut pas l'indisponibilité (de parties) du réseau Internet et l'indisponibilité de l'infrastructure locale du demandeur du service.

Au niveau interne, le CA archive les éléments, données et documents suivants relatifs à son service: CRL et delta CRL. Les CRL et delta CRL sont archivées pendant une période d'au moins 30 jours suivant leur publication.

4.11 Dépôt et récupération de clés

Fiducie et récupération de clés pas autorisées.

5. CONTROLES ADMINISTRATIFS, OPERATIONNELS ET PHYSIQUES

Ce chapitre décrit les contrôles de sécurité non techniques utilisés par le CA et les autres partenaires PKI, dans le cadre des opérations de génération de clé, d'authentification de la personne concernée, de délivrance du certificat, de révocation de certificat, d'audit et d'archivage.

5.1 Contrôles de sécurité physiques

Le CSP met en œuvre des contrôles physiques sur son site. Les contrôles physiques de l'opérateur du CSP comprennent les aspects suivants:

- Les locaux sécurisés de l'opérateur du CSP sont situés à un endroit approprié pour les opérations hautement sécurisées. Ces locaux comprennent des zones numérotées et des pièces, des cages, des coffres-forts et des armoires verrouillables.
- L'accès physique est restreint par la mise en œuvre de mécanismes qui contrôlent le passage d'une zone à une autre, ou l'accès aux zones hautement sécurisées, comme la localisation des opérations CSP dans une salle informatique sécurisée, surveillée physiquement et protégée par des alarmes de sécurité et un système impliquant que tout mouvement d'une zone à une autre s'effectue avec un jeton et des listes de contrôle d'accès.
- Fonctionnement redondant de l'alimentation électrique et de la climatisation.
- Les locaux sont protégés contre l'inondation.
- Le CSP met en œuvre des mesures de prévention, de protection et de lutte contre l'incendie.
- Les équipements sont entreposés en toute sécurité. Les équipements de back up sont stockés à un autre endroit, protégé physiquement contre les l'incendie et l'inondation.
- Pour prévenir toute diffusion indésirable des données sensibles, les déchets sont évacués de manière sécurisée.
- Le CSP réalise le back up partiellement hors site.

Les sites CSP hébergent l'infrastructure nécessaire pour fournir les services CA. Les sites CA mettent en œuvre les contrôles de sécurité adéquats, y compris le contrôle d'accès, la détection des intrusions et la surveillance. L'accès aux sites est limité au personnel autorisé repris sur la liste de contrôle d'accès, qui doit faire l'objet d'un audit.

Un contrôle d'accès très strict est mis en œuvre partout où il y a du matériel et des infrastructures hautement sensibles, y compris le matériel et les infrastructures destinés à la signature des certificats, aux CRL et delta CRL, aux OCSP et aux archives.

5.2 Contrôles des procédures

Le CSP applique des procédures, en matière de personnel et de management, qui offrent une garantie raisonnable de la fiabilité et de la compétence des membres de l'équipe et de réalisation satisfaisante de leurs tâches dans le domaine des technologies de la signature électronique.

Le CSP fait signer à chaque membre de l'équipe une déclaration d'absence de conflit d'intérêt avec le CSP, de respect de la confidentialité et de protection des données personnelles.

Tous les membres de l'équipe qui assument des fonctions de gestion des clés, les administrateurs, le personnel de sécurité et les auditeurs de système ou de toute autre opération pouvant affecter matériellement ces opérations sont considérés comme occupant des postes de confiance. Le CSP mène une enquête initiale pour tous les membres de l'équipe qui sont candidats pour une position de confiance en vue de déterminer le degré de fiabilité et de compétence.

Lorsqu'un double contrôle est requis, au moins deux personnes occupant une position de confiance doivent apporter leurs connaissances respectives et séparées pour procéder aux opérations courantes.

Le CSP fait en sorte que toutes les actions concernant le CSP puissent être attribuées au système du CSP et au membre de l'équipe CSP qui a réalisé l'action.

Pour les fonctions CSP critiques, le CSP met en œuvre un double contrôle.

Le CSP distingue les groupes de travail suivants:

- personnel d'exploitation CSP qui gère les opérations pour les certificats.
- personnel administratif qui s'occupe de la plate-forme de support du CSP.
- personnel de sécurité qui met en œuvre les mesures de sécurité

5.3 Contrôles de sécurité du personnel

Le CSP met en œuvre des contrôles de sécurité pour les tâches et les performances des membres de son équipe. Ces contrôles de sécurité sont exposés dans une politique et comprennent les éléments suivants :

5.3.1 Qualifications, Expérience, Autorisations

Le CSP effectue des contrôles pour définir les antécédents, les qualifications et l'expérience nécessaires pour fonctionner dans le domaine de compétence du job spécifique. Ces vérifications d'antécédents comprennent:

- Condamnations pour les délits graves;
- Fausses déclarations du candidat;
- Exactitude des références; • Les autorisations, le cas échéant.

5.3.2 Vérifications des antécédents et procédures d'autorisation

Le CSP effectue les contrôles nécessaires pour les employés potentiels au moyen de rapports de situation fournis par une autorité compétente, des déclarations de parties tierces ou des déclarations personnelles signées.

5.3.3 Besoins et procédures de formation

Le CSP offre au personnel des formations pour que celui-ci puisse assumer ses fonctions CA.

5.3.4 Période et procédures de recyclage

Des recyclages périodiques sont également prévus pour assurer la continuité et l'actualisation des connaissances du personnel et des procédures.

5.3.5 Rotation des jobs Sans objet.

5.3.6 Sanctions à l'encontre du personnel

Le CSP sanctionne le personnel pour toute action non autorisée, abus d'autorité et usage non autorisé des systèmes dans le but d'imposer une responsabilité au personnel CSP, le cas échéant.

5.3.7 Contrôle des contractants indépendants

Les sous contractants indépendants du CSP et leur personnel font l'objet des mêmes contrôles de contexte que le personnel CSP. Les vérifications des antécédents comprennent:

- Condamnations pour les délits graves;
- Fausses déclarations du candidat;
- Exactitude des références;
- Les autorisations, le cas échéant; • Protection de la confidentialité;
- Conditions de confidentialité.

5.3.8 Documentation pour la formation initiale et le recyclage

Le CSP met à la disposition du personnel la documentation nécessaire durant la formation initiale, le recyclage ou autrement.

5.4 Procédures de journalisation d'audit

Les procédures pour la journalisation d'audit comprennent la journalisation d'événements et l'audit des systèmes, dans le but de maintenir un environnement sécurisé. Le CSP met en œuvre les contrôles suivants:

Le système de journalisation d'événements CA consigne les événements tels que, notamment:

- Emission d'un certificat;
- Révocation d'un certificat;
- Suspension d'un certificat;
- La réactivation d'un certificat ;
- Révocation automatique;
- Publication d'une CRL ou delta CRL.

Le CSP audite tous les enregistrements du journal d'événement. Les enregistrements du rapport d'audit comportent:

- L'identification de l'opération;
- La date et l'heure de l'opération;
- L'identification du certificat, impliqué dans l'opération;
- L'identité du demandeur de la transaction.

En outre, le CSP conserve les journaux internes et les rapports d'audit des événements opérationnels importants dans l'infrastructure. Il s'agit notamment:

- Du démarrage et de l'arrêt des serveurs;

- Des pannes et des problèmes majeurs;
- De l'accès physique du personnel et d'autres personnes aux parties sensibles du site CSP;
- Du back up et des récupérations;
- Du rapport des tests de remise en service après catastrophe;
- Des inspections d'audit;
- Des extensions et changements des systèmes, logiciels et infrastructure;
- Des intrusions et tentatives d'intrusion dans les zones sécurisées.

Autres documents nécessaires pour les audits, notamment:

- Plans et descriptions de l'infrastructure;
- Plans et descriptions des sites;
- Configuration du matériel et des logiciels;
- Listes de contrôle d'accès du personnel.

Le CSP veille à ce que le personnel désigné à cet effet vérifie les fichiers journaux à intervalles réguliers et rapporte les événements anormaux.

Les fichiers journaux et les rapports d'audit sont archivés pour inspection par le personnel autorisé du CA, les RA et les auditeurs désignés. Les fichiers journaux doivent être protégés de façon adéquate par un mécanisme de contrôle d'accès. Les fichiers journaux et les rapports d'audit font l'objet d'un back up.

Les événements d'audit ne donnent pas lieu à une consignation dans le journal.

5.5 Archivage des dossiers

Le CSP conserve en interne les dossiers des éléments suivants:

- Tous les certificats pendant une période d'au moins 30 ans après expiration du certificat;
- Journaux d'audit de l'émission des certificats pour une période d'au moins 30 ans après émission du certificat;
- Journal d'audit de la révocation d'un certificat d'au moins 30 ans après révocation du certificat;
- CRL et Delta CRL d'au moins 30 ans après leur publication;
- Le CSP doit conserver le dernier back up des archives CA d'au moins 30 ans après émission du dernier certificat.

Le CA conserve les archives dans un format consultable.

Le CA veille à l'intégrité des dispositifs de stockage physique et met en œuvre des mécanismes de copie adéquats pour éviter toute perte de données.

Les archives sont accessibles au personnel autorisé du CA et au RA.

5.5.1 Types de dossiers

Le CSP conserve d'une manière fiable les dossiers des certificats numériques, données d'audit, informations et documentation des systèmes CSP.

5.5.2 Période de conservation

Le CSP conserve d'une manière fiable les dossiers des certificats numériques pendant la durée mentionnée à l'article 5.5 de ce CPS.

5.5.3 Protection des archives

Seul le gestionnaire des dossiers (membre de l'équipe chargée de la conservation des dossiers) peut accéder aux archives CSP. Des mesures doivent être prises pour assurer:

- La protection contre la modification des archives, comme l'entreposage des données sur un support non réinscriptible;
- La protection contre la suppression des archives;
- La protection contre la détérioration des médias sur lesquels les archives sont stockées, comme le transfert régulier des données sur des médias non utilisés.

Le CSP agit conformément à l'application potentielle par l'Autorité Fédérale Belge de la procédure de l'article 14 de la Loi du 8 août 1983 et l'article 7 de la loi du 12 mai 1927. Dans une telle occurrence, le CA agit conformément aux instructions fournies par la personne désignée par l'Arrêté Royal pour ce qui concerne les données faisant partie des cartes pour étrangers et des certificats.

5.5.4 Procédures de back up des archives

Un back up différentiel des archives du CA est effectué quotidiennement les jours ouvrables.

5.5.5 Condition d'horodatage sur les dossiers Sans objet.

5.5.6 Collecte des archives

Le système de collecte des archives du CA est interne.

5.5.7 Procédures d'obtention et de vérification des informations d'archivage

Seuls les membres de l'équipe CA ayant un contrôle hiérarchique clair et une description de job définie peuvent obtenir et vérifier les informations d'archivage.

Le CA conserve les dossiers en format électronique ou sur papier.

5.6 Changement de clé

Sans objet.

5.7 Récupération de compromission et de catastrophe

Dans un document interne distinct, le CA spécifie les procédures de rapport et de traitement des incidents et des compromissions. Le CA spécifie les procédures de récupération utilisées si les ressources informatiques, les logiciels et/ou les données sont corrompus ou suspectés de corruption.

Le CA définit les mesures nécessaires pour assurer une récupération complète et automatique en cas de catastrophe, de corruption des serveurs, des logiciels ou des données.

Un plan de continuité des opérations a été élaboré pour assurer la continuité des opérations suite à une catastrophe naturelle ou autre.

Toutes ces mesures sont conformes à ISO 1-7799.

Le CA établit:

- Les ressources de récupération en cas de catastrophe dans deux endroits, suffisamment distants l'un de l'autre;
- Une communication rapide entre les deux sites pour assurer l'intégrité des données;

- Une infrastructure de communication des deux sites vers le RA supportant les protocoles de communication sur Internet ainsi que les protocoles de communication utilisés par l'administration publique belge.
- Les infrastructures et procédures de récupération après catastrophe sont testées au moins chaque année.

5.8 Résiliation du CA

Dès l'instant où le CA reçoit la notification par l'Autorité Fédérale Belge que son contrat va s'achever et/ou dès le moment où son contrat est annulé prématurément, le CA consulte l'État belge pour déterminer les étapes requises pour (1) garantir une transition aisée pour la prestation des services au nouveau CA, et pour (2) assurer la destruction, la suppression, la restitution et/ou la sécurité de l'information, des données à caractère personnel et des fichiers reçus par le CA dans le cadre de sa mission de CA.

6. CONTROLES DE SECURITE TECHNIQUE

Ce chapitre définit les mesures de sécurité que le CA prend pour protéger ses clés cryptographiques et les données d'activation (ex. PIN, mots de passe ou parts de clés détenues manuellement).

6.1 Génération et installation de la paire de clés

Le CA protège sa (ses) clé(s) privée(s) conformément à ce CPS. Le CA utilise des clés de signature privées uniquement pour signer les certificats, les CRL, les Delta CRL et réponses OCSP en conformité avec l'usage prévu pour chacune de ces clés.

Le CA s'abstient d'utiliser ces clés privées du CA autrement que dans la portée du domaine du « Foreigner CA ».

6.1.1 Procédure de génération de clé privée CA

Le CA utilise une procédure fiable pour la génération de sa clé privée racine selon une procédure documentée. Le CA distribue les parts de secret de sa (ses) clé(s) privée(s). Le CSP a l'autorité pour transférer ces parts de secret aux détenteurs de parts de secret selon une procédure documentée.

6.1.1.1 Utilisation de la clé privée CA

La clé privée du « Foreigner CA » est utilisée pour signer les certificats délivrés, les listes de révocation des certificats et les certificats OCSP. Les autres usages sont limités.

6.1.1.2 Type de clé privée CA

Pour sa clé racine, le CA (Belgium Root CA) utilise l'algorithme RSA SHA-1 avec une longueur de clé de 2048 bits.

La première clé privée du Belgium Root CA est certifiée pour une période allant du 27 janvier 2003 au 27 janvier 2014.

Pour sa clé principale, le « Foreigner CA » utilise l'algorithme RSA SHA-1 avec une longueur de clé de 2048 bits. La première clé privée « Foreigner CA » est certifiée pour une période de validité du 27 janvier 2003 au 27 juin 2009. Les nouvelles clés privées du « Foreigner CA » seront certifiées pour 6 ans. Une nouvelle remplacera la clé active avant que la période de validité de la clé active ne chute en dessous de 5 ans.

6.1.2 Génération de la clé CA

Le CA génère et protège de manière sécurisée la (les) clé(s) privée(s) en utilisant un système fiable et prend les précautions nécessaires pour prévenir la compromission ou l'usage non autorisé de sa (ses) clé(s) privée(s). Le processus est surveillé par des représentants de l'Autorité Fédérale Belge pour assurer une exécution adéquate et sûre de la procédure de génération de la clé CA. Le CA met en œuvre des procédures en ligne avec ce CPS. Le CA accepte les normes publiques, internationales et européennes applicables à la fiabilité des systèmes. Au moins trois personnes occupant une position de confiance participent à la génération et à l'installation de la (des) clé(s) privée(s) CA.

6.2 Régénération et réinstallation de la paire de clés

Lorsque la (les) clé(s) secrète(s) est (sont) remplacée(s) par de nouvelles, le CA doit utiliser exactement la même procédure que pour la première. Le CA doit immédiatement mettre hors service et détruire les clés utilisées dans le passé ainsi que les dispositifs infalsifiables et toutes les copies de back up de ses clés privées dès qu'elles sont disponibles.

6.2.1 Dispositifs de génération de la clé du CA

La génération de la clé privée du « Foreigner CA » s'effectue avec un dispositif cryptographique sécurisé répondant aux conditions requises, incluant FIPS 140-1 niveau 3.

La génération de la clé privée du CA nécessite le contrôle de plusieurs membres autorisés de l'équipe CA occupant des postes de confiance, et d'au moins un représentant de l'Autorité Fédérale Belge. Plusieurs membres de la direction du CA donnent par écrit l'autorisation de générer des clés.

6.2.2 Stockage de la clé privée du CA

Le CA utilise un dispositif cryptographique sécurisé pour stocker sa propre clé privée, conformément aux exigences FIPS 140-1 niveau 3.

6.2.2.1 Contrôles du stockage de la clé du CA

Le stockage de la clé privée du CA nécessite de multiples contrôles par des membres autorisés du personnel CSP occupant des postes de confiance. Plusieurs membres de la direction du CSP donnent les autorisations par écrit pour le stockage de la clé et le personnel autorisé.

6.2.2.2 Back up de la clé du CA

La (les) clé(s) privée(s) du CA fait (font) l'objet d'un back up, est (sont) entreposée(s) et récupérée(s) par des membres autorisés du personnel CSP occupant des postes de confiance. Plusieurs membres de la direction du CSP donnent les autorisations par écrit pour le stockage de la clé et le personnel autorisé.

6.2.2.3 Parts de secret

Les parts de secret CA sont détenues par plusieurs titulaires autorisés pour sauvegarder et améliorer la fiabilité des clés privées. Le CA entrepose la (les) clé(s) privée(s) dans plusieurs dispositifs infalsifiables. Au moins trois membres du CSP doivent agir conjointement pour activer la clé privée du CA.

Les clés privées du CA ne peuvent pas être entiercées. Le CSP met en œuvre des mesures de récupération en cas de catastrophe interne.

6.2.2.4 Acceptation des parts de secret

Avant que les détenteurs de parts de secret acceptent une part de secret, ils doivent avoir personnellement observé la création, la recréation et la distribution de la part ou sa chaîne de possession.

Le détenteur de part de secret reçoit la part de secret par le biais d'un support physique, comme un module cryptographique matériel approuvé par le CA. Le CA conserve des enregistrements écrits de la distribution des parts de secret.

6.2.3 Distribution de la clé privée du CA

Le CA documente la distribution de sa propre clé privée. Si les conservateurs des tokens doivent être remplacés dans leur rôle, le CA conserve une trace de la nouvelle distribution des tokens.

6.2.4 Destruction de la clé privée du CA

A la fin de leur durée de vie, les clés privées du CA sont détruites par au moins trois membres de l'équipe du CSP occupant une position de confiance en présence d'un représentant de l'Autorité Fédérale Belge, afin de garantir que les clés privées ne puissent pas être récupérées et réutilisées. Les clés du CA sont détruites en déchiquetant leur support de stockage principal et de back up, et détruisant et en déchiquetant leurs parts et en détruisant en désactivant et en retirant définitivement les modules matériels sur lesquels les clés sont conservées.

Le processus de destruction des clés est documenté et tous les dossiers associés sont archivés.

6.3 Protection de la clé privée et contrôles du module cryptographique

Le CA utilise des dispositifs cryptographiques appropriés pour réaliser les tâches de gestion de clé du CA. Ces dispositifs cryptographiques s'appellent les Hardware Security Modules (HSMs). Ces dispositifs répondent aux conditions du FIPS 140-1 Niveau 3 ou plus, qui garantit, entre autres choses, que toute tentative de violation du dispositif est immédiatement détectée et que les clés privées ne peuvent pas laisser les dispositifs non cryptés.

Les mécanismes matériels et logiciels qui protègent les clés privées du CA sont documentés.

Les HSM ne quittent pas l'environnement sécurisé du site du CA. Si les HSM ont besoin d'être entretenus ou réparés, ce qui ne peut être fait sur le site du CA, ils doivent être envoyés en toute sécurité au fabricant. La (les) clé(s) privée(s) du CA n'est (ne sont) pas présente(s) sur les HSM lorsqu'ils sont envoyés pour entretien à l'extérieur du site sécurisé du CA. Entre les sessions d'utilisation, les HSM sont conservés dans le site sécurisé du CA.

La clé privée du CA reste sous le contrôle de 3 personnes parmi 5 possibles.

La clé privée du CA n'est pas entiercée.

A la fin de l'opération de génération de clés, les nouvelles clés CA sont gravées et encryptées sur un CD-ROM (stockage du back up de la clé). Le CA enregistre chaque étape du processus de back up de la clé en utilisant une forme spécifique de consignation de l'information.

La clé privée du CA est archivée localement dans les sites du CA.

Des gardiens CA sont chargés d'activer et de désactiver la clé privée. La clé est alors active pour une période définie.

La clé privée du CA peut être détruite à la fin de sa durée de vie.

6.4 Autres aspects de la gestion de la paire de clés

Le CA archive sa (ses) propre(s) clé(s) publique(s)). Le CA émet des certificats avec les périodes de validité telles qu'indiquées sur les certificats.

6.4.1 Corruption des ressources informatiques, logiciels, et/ou données

Le CA prend les mesures nécessaires pour assurer la récupération complète et automatique du service en cas de catastrophe, de corruption des serveurs, des logiciels ou des données. Toutes ces mesures sont conformes à la norme ISO 1-7799.

Le CA localise ses ressources de récupération en cas de catastrophe à une distance suffisante des ressources principales pour éviter qu'une catastrophe puisse corrompre les ressources des deux côtés. Le CA établit des communications suffisamment rapides entre les deux sites pour garantir l'intégrité des données. Le CA établit une infrastructure de communication sécurisée des deux sites vers le RA, Internet et les réseaux de l'Administration publique.

Le CA prend les mesures nécessaires pour tester l'infrastructure et les procédures de récupération en cas de catastrophe au moins une fois par an sans interruption ni dégradation du service.

6.4.2 Révocation de la clé publique du CA

Si la clé publique du « Foreigner CA » est révoquée, le CA doit immédiatement:

- Avertir toutes les autorités de certification impliquées dans la certification.
- Avertir le RA.
- Avertir le grand public par différents moyens, dont:
  - o Un message sur le site web du CA. o Un communiqué de presse dans les médias belges. o Des annonces dans les principaux journaux belges.
- Lister le certificat du « Foreigner CA » dans les CRL et les delta CRL.
- Actualiser le statut du certificat dans le service interface du web.
- Révoquer tous les certificats signés avec le certificat révoqué.
- Après avoir évalué les raisons de la révocation et pris des mesures pour éviter la cause de la révocation dans le futur, et après avoir obtenu l'autorisation du RA, le CA peut:
- Générer une nouvelle paire de clés et certificat associé.
- Réémettre tous les certificats révoqués.

6.4.3 Compromission de la clé privée du CA

Si la clé privée du CA est compromise, le certificat correspondant doit immédiatement être révoqué. Le CA prend en outre toutes les mesures décrites sous 6.4.2.

6.5 Données d'activation

Le CA stocke et archive en toute sécurité les données d'activation associées à sa propre clé privée et ses opérations.

6.6 Contrôles de la sécurité informatique

Le CA met en œuvre certains contrôles de sécurité informatique.

6.7 Contrôles de sécurité du cycle de vie

Le CA effectue régulièrement des contrôles de développement et des contrôles sécuritaires.

6.8 Contrôles de sécurité du réseau

Le CA assure la sécurité des systèmes, y compris des pare-feu. Les intrusions sur le réseau sont surveillées et détectées. En particulier:

Toutes les communications entre le CA et l'opérateur RA concernant n'importe quelle phase du cycle de vie du certificat sont sécurisées par un encryptage PKI et des techniques de signature pour assurer la confidentialité et l'authentification mutuelle, dont notamment les communications concernant les demandes de certificat, émission, suspension, levée de suspension et révocation.

Le site web du CA fournit des connexions encryptées par le biais du protocole Secure Socket Layer (SSL) et une protection anti-virus.

Le réseau du CA est protégé par un mur pare-feu et un système de détection des intrusions.

Il est interdit d'accéder aux ressources sensibles du CA, y compris les bases de données CA externes au réseau de l'opérateur CA.

Les sessions Internet pour la demande et la fourniture d'informations sont encryptées.

7. CERTIFICAT ET PROFILS CRL

Ce chapitre présente le format du certificat, du CRL et les formats OCSP.

7.1 Profil du certificat

7.1.1 Certificat d'identité

La description des champs pour ce certificat est fournie dans le tableau ci-dessous. Les pseudonymes ne peuvent pas être utilisés dans ce certificat.

Foreigner Authentication Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 5 years and 3 months[13]	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Foreigner CA	Fixed
SerialNumber		X		<yyyy><ss>[14]	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic

[13] maximum certificate validity period, shorter certificate validity periods can be applied

[14] corresponding CA certificate only based on this field.

<yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find

serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under BRCA(1) 2.16.56.1.1.1.7.2 Certificates issued under BRCA2 2.16.56.9.1.1.7.2	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
					Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
digitalSignature				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidf<yyyy><ss>[15].crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslClient - smime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		Certificates issued under BRCA(1) http://certs.eid.belgium.be/belgiumrs.crt Certificates issued under BRCA2 http://certs.eid.belgium.be/belgiumrs2.crt	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

7.1.2 Certificat pour signature numérique

La description des champs pour ce certificat est fournie dans le tableau ci-dessous. Les pseudonymes ne peuvent pas être utilisés dans ce certificat.

Foreigner Signature Certificate

[15] <yyyy> represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field

<yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find

Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 5 years and 3 months[16]	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Foreigner CA	Fixed
SerialNumber		X		<yyyy><ss>[17]	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under the BRCA(1) 2.16.56.1.1.1.7.1 Certificates issued under the BRCA2 2.16.56.9.1.1.7.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
Qualified Certificate Statement					
qcStatement	{ id-etsi-qcs 1 }	X		0.4.0.1862.1.1	

[16] maximum certificate validity period, shorter certificate validity periods can be applied.

[17] corresponding CA certificate only based on this field.

<yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find

KeyUsage	{id-ce 15}	X	TRUE	N/a	
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidf<yyyy><ss>[18].crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sMime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		Certificates issued under the BRCA(1) http://certs.eid.belgium.be/belgiumrs.crt Certificates issued under the BRCA2 http://certs.eid.belgium.be/belgiumrs2.crt	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

7.1.3 Certificat “Foreigner CA”

Ce certificat est émis par le BRCA pour identifier le CA au moyen d’un certificat numérique. La description des champs pour ce certificat est fournie dans le tableau ci-dessous.

Foreig er CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					

[18] corresponding CA certificate only based on this field.
<yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find

Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years and 8 months	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Certificate issued under the BRCA(1): Belgium Root CA Certificates issued under the BRCA2: Belgium Root CA2	Fixed
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Foreigner CA	Fixed
SerialNumber		X		<yyyy><ss>	
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under the BRCA(1): 2.16.56.1.1.7.2 Certificates issued under the BRCA2: 2.16.56.9.1.7.2	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
CrlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
DistributionPoint					
FullName		X		Certificates issued under the BRCA(1): http://crl.eid.belgium.be/belgium.crl Certificates issued under the BRCA2: http://crl.eid.belgium.be/belgium2.crl	Fixed

BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			SslCA – smimeCA – ObjectSigning CA	Fixed

7.2 Profil CRL

Conformément à IETF PKIX RFC 2459, le CA supporte les CRL conformes à:

- Numéros de version supportés pour les CRL.
- Extensions d'entrée CRL et CRL peuplées et leur degré de criticité.

Le profil de la liste de révocation de certificats est présenté dans le tableau ci-dessous:

Version	v2
Signature	sha1RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time>+7 days
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>
CrlEntryExtensions	
CRL Reason Code	Certificate Hold(6) (for suspended certificates) Note: Otherwise NOT included!
CrlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <CA assigned unique number>

Le profil de la liste de révocation de certificats delta est présenté dans le tableau ci-dessous:

Version	v2
signature	sha1RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time+7 days >
RevokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	

CRL Reason Code	Certificate Hold(6) (for suspended certificates) removeFromCrl(8) (to unsuspend certificates) Note: Otherwise NOT included!
crlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <CA assigned unique number>
Delta CRL Indicator	<base CRL Number>

Les CRL et delta CRL du CA supportent les champs et les extensions spécifiés au chapitre 5 du RFC 2459: "Infrastructure à clés publiques Internet X.509 et profil CRL".

7.3 Profil OCSP

Le profil OCSP suit IETF PKIX RFC2560 OCSP v1. Aucune extension OCSP n'est supportée. Le CA supporte les requêtes multiples de statut de certificat dans une requête OCSP du moment qu'elles sont signées par le même CA. La réponse OCSP est signée par une clé secrète dont la clé publique concordante est certifiée par toutes les autorités de certification « Foreigner CA ».

Ce certificat est émis par la racine CA du l'Autorité Fédérale Belge pour certifier les répondants OCSP. La description des champs pour ce certificat est fournie dans le tableau ci-dessous.

Belgium OCSP Responder					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Generated by the CA at Key Generation Process Time	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 1 Year and 3 months	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		[Issuing CA]	Fixed
SerialNumber		X		<yyyy><ss>[19]	
Subject					

[19] <yyyy>: est l'année où le CA est utilisé pour la première fois, par ex. 2006; <ss>: numéro de série unique utilisé en support d'applications pour rechercher des certificats CA en utilisant uniquement ce champ.

CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }			Belgium OCSP Responder	Fixed
Standard Extensions	OID	Include	Critical	Value	
KeyUsage	{id-ce 15}	X	TRUE	N/a	
DigitalSignature				Set	Fixed
enhancedKeyUsage			FALSE		
ocspSigning	1.3.6.1.5.5.7.3.9	X			
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
ocspNoCheck	{ id-pkix-ocsp 5 } 1.3.6.1.5.5.7.48.1.5		FALSE		
Null		X			

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

En ce qui concerne le Certificat Qualifié pour signatures électroniques, le CSP procède selon les termes de la loi du 9 juillet 2001 qui définit le cadre légal des signatures électroniques en Belgique. Le CA répond aux exigences définies dans les documents de politique ETSI qui se réfèrent aux certificats qualifiés, y compris:

- les exigences politiques TS 101 456 pour les autorités de certification qui émettent des certificats qualifiés;
- le profil de certificat qualifié TS 101 862.

En ce qui concerne le certificat d'identité, le CSP répond aux exigences définies dans les documents de politique ETSI qui se réfèrent aux certificats à clés publiques, y compris :

- les exigences politiques TS 101 042 pour les autorités de certification qui émettent des certificats à clés publiques (niveau standardisé).

Le CSP accepte les audits de conformité afin de s'assurer qu'il respecte les exigences, normes, procédures et niveaux de service conformément à ce CPS. Le CSP accepte cette vérification de ses propres pratiques et procédures qu'il ne divulgue pas publiquement sous certaines conditions, comme la confidentialité, les secrets commerciaux etc. De tels audits peuvent être réalisés directement ou via un agent par :

- l'autorité de supervision des prestataires de services de certification en Belgique qui agit sous l'autorité du l'Autorité Fédérale Belge.
- L'Autorité Fédérale Belge ou une tierce partie désignée par l'Autorité Fédérale Belge

Le CSP évalue les résultats de ces audits avant de les mettre en application.

Pour réaliser les audits, un auditeur indépendant sera désigné; cet auditeur ne sera pas affilié directement ou indirectement, de quelque manière que ce soit, au CSP ou à tout CA, et n'aura aucun intérêt conflictuel.

L'audit aborde les aspects suivants:

- Conformité des principes et des procédures du CSP avec les procédures et les niveaux de service définis dans le CPS;
- Gestion des infrastructures qui mettent en oeuvre les services CSP;

- Gestion des infrastructures physiques sur site.
- Adhésion au CPS;
- Respect des lois belges afférentes;
- Respect des niveaux de service convenus;
- Inspection des rapports d'audit, des registres, des documents pertinents etc ;
- Cause de toute non-conformité aux conditions reprises ci-dessus.

Si des irrégularités sont détectées, le CSP soumettra un rapport à l'auditeur, mentionnant les mesures qui seront prises pour rectifier la situation et garantir la conformité. Si les mesures proposées sont considérées comme insuffisantes, un second audit sera réalisé pour garantir la conformité.

Certipost NV est conforme à la version actuelle des exigences de base pour la délivrance et la gestion des certificats publiquement approuvés («Baseline Requirements») publiée sur le site http://www.cabforum.org. En cas d'incompatibilité entre ce document et ces Exigences, ces Exigences ont préséance sur ce document.

9. AUTRES POINTS ET CONSIDERATIONS JURIDIQUES

9.1 Honoraires

La loi sur les cartes d'identité réglemente les honoraires dus par l'étranger pour les certificats sur sa carte pour étranger.

Le CA ne facture aucun honoraire pour la publication et l'extraction de ce CPS.

Le CA fournira gratuitement les services suivants:

- Délivrance, publication et renouvellement des certificats;
- Révocation des certificats;
- Suspension des certificats;
- Publication des CRLs et des Delta CRLs.

L'Autorité Fédérale Belge peut accéder gratuitement aux ressources suivantes.

- services de vérification d'état OCSP.
- Téléchargement des CRL et delta CRL.
- Service de vérification d'état du certificat.
- Service de répertoire de certificat.

Au moyen de procédures dédiées, le CA met gratuitement à la disposition de chaque utilisateur individuel les services suivants qui peuvent faire l'objet d'une demande:

Service	Gratuit
Services de vérification d'état OCSP	10 demandes par utilisateur par jour
Téléchargement de CRL	1 téléchargement par utilisateur par semaine
Téléchargement d'une delta CRL	8 téléchargements par utilisateur par jour
Service de répertoire certificat	30 téléchargements par semaine
Enoncé des Pratiques de Certification	2 téléchargements par utilisateur par jour

Le CA met en œuvre des mécanismes qui visent à protéger ces services de tout abus. Tout accès au-delà des limites spécifiées peut faire l'objet d'une facturation d'honoraires envoyée directement à l'utilisateur par le CSP dans le cadre du contrat CSP avec l'Autorité Fédérale Belge.

9.2 Responsabilité

La responsabilité du CSP à l'égard de l'abonné ou d'une partie confiante est limitée au paiement de préjudices s'élevant à 2500 € par transaction, affectée par les événements repris dans la section 9.2.1.

9.2.1 Certificats qualifiés

En ce qui concerne la délivrance de certificats qualifiés pour signatures électroniques (certificat de signature), l'article 14 de la loi sur les signatures électroniques régit la responsabilité du CSP.

Conformément à cette disposition, le CSP est responsable du préjudice causé à tout organisme ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de :

(a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;

(b) l'assurance que, au moment de la délivrance du certificat qualifié, le signataire identifié dans le certificat qualifié détenait la clé privée correspondant à la clé publique donnée ou identifiée dans le certificat;

(c) l'assurance que la clé privée et la clé publique peuvent être utilisées de façon complémentaire;

Le CSP est responsable de tout préjudice causé à tout organisme ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat sauf si le CSP prouve qu'il n'a commis aucune négligence.

9.2.2 Certificats qui ne peuvent pas être considérés comme des certificats qualifiés

Les règles générales en matière de responsabilité s'appliquent à tout préjudice causé à un organisme ou personne physique ou morale qui se fie raisonnablement à un certificat délivré par le CSP.

Le CSP décline explicitement toute responsabilité à l'égard de parties confiantes dans tous les cas où le certificat d'identité est utilisé dans le contexte d'applications permettant l'utilisation du certificat d'identité pour la génération de signatures électroniques.

9.3 Confidentialité des informations

Dans le cadre des services effectués, le CA et l'opérateur RA (RRN) agissent en tant que “processeurs” de données à caractère personnel en conformité avec l'article 16 de la loi du 8 décembre 1992, alors que les administrations communales agissent en tant que “contrôleurs” pour le traitement des données à caractère personnel.

Le CSP respecte les réglementations relatives aux données à caractère personnel comme décrit dans ce CPS. Les informations confidentielles englobent :

- toute information personnelle identifiable sur des étrangers, autres que celles reprises dans un certificat.
- le motif exact pour la révocation ou la suspension d'un certificat.
- les rapports d'audit.
- les informations consignées à des fins de reporting, tels que des enregistrements de requêtes par la RA.
- la correspondance relative aux services CA.
- la(les) clé(s) privée(s) CA .

Les éléments suivants ne sont pas des informations confidentielles:

- les certificats et leur contenu.
- l'état d'un certificat.

Le CSP ne divulgue pas, ni n'est tenu de divulguer, des informations confidentielles sans une demande authentifiée et justifiée spécifiant :

- la partie envers laquelle le CA est tenu au devoir de garder l'information confidentielle. Le CA est tenu à une telle obligation envers la RA et répond promptement à toute demande de ce type;
- un ordre du tribunal.

Dans le cadre du Contrat Cadre entre le CSP et l'Autorité Fédérale Belge, le CSP peut facturer des frais administratifs pour procéder à de telles divulgations d'informations.

Les parties qui demandent et reçoivent des informations confidentielles reçoivent la permission à condition qu'elles les utilisent aux fins requises, qu'elles les sécurisent contre toute compromission, et s'abstiennent de les utiliser ou de les divulguer à des tiers.

Ces parties sont également tenues d'observer les règles régissant la protection des données à caractère personnel en conformité avec la loi.

9.3.1 Conditions de divulgation

Des informations non confidentielles peuvent être divulguées à tous les étrangers et partie confiante aux conditions ci-après:

- l'état d'un certificat unique est fourni sur demande d'un étranger ou d'une partie confiante;
- les étrangers peuvent consulter des informations non confidentielles que le CSP détient à leur sujet.

Les informations confidentielles ne seront pas divulguées par le CSP aux étrangers, ni aux parties confiantes à l'exception des informations: • sur eux-mêmes;

- sur des personnes dont ils ont la garde.

Seule la RA est autorisée à accéder aux informations confidentielles.

Le CSP gère en bonne et due forme la divulgation d'informations au personnel CSP.

Le CA s'authentifie à l'égard de toute partie qui demande la divulgation d'informations par :

- la présentation d'un certificat d'authentification à la demande de l'étranger ou de la partie confiante
- la signature des réponses aux demandes OCSP, aux CRLs et delta CRLs.

Le CA crypte toutes les communications d'informations confidentielles, y compris:

- le lien de communication entre le CA et la RA;
- les sessions visant à fournir les certificats.

Outre les informations conservées par le CSP, la RA conserve également des informations relatives aux certificats, plus spécifiquement dans le registre des cartes pour étranger. La loi sur le registre national réglemente l'accès au registre des cartes pour étrangers et à d'autres données sur les étrangers qui sont détenus par le RRN.

9.3.2 Protection des informations personnelles

Le CSP agit dans les limites de la loi belge du 8 décembre 1992 sur la protection de la vie privée à l'égard du traitement des données à caractère personnel telle que modifiée par la loi du 11 décembre 1998 transposant la directive européenne 1995/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le CSP reconnaît également la directive européenne 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Le CSP ne conserve pas d'autres données sur les certificats ou les étrangers autres que les données qui lui ont été transmises et autorisées par la RA. Sans le consentement de la personne concernée ou l'autorisation explicite par la loi, les données à caractère personnel traitées par le CSP ne seront pas utilisées à d'autres fins.

9.3.3 Droits de propriété intellectuelle

L'État belge détient et se réserve tous les droits de propriété intellectuelle associés à ses propres bases de données, ses sites web, les certificats numériques CA et toute autre publication, quelle qu'elle soit , provenant du CSP, y compris le présent CPS.

Le CSP détient et se réserve tous les droits de propriété intellectuelle qu'il détient sur ses propres infrastructures, bases de données, site web, etc.

Les logiciels et la documentation développés par le CSP dans le cadre du projet de carte pour étranger sont la propriété exclusive de l'État belge.

9.4 Représentations et garanties

Toutes les parties dans le domaine du CSP, en ce compris le CA lui-même, la RA, les LRA et les étrangers, garantissent l'intégrité de leur(s) clé(s) privée(s) respective(s). Si une desdites parties soupçonne qu'une clé privée a été compromise, elle informera immédiatement son LRA (municipalité), la police ou le Helpdesk RA.

9.4.1 Obligations de l' étranger

Sauf mention contraire dans le CPS, les obligations de l' étranger comprennent les obligations suivantes :

- s'abstenir de falsifier un certificat.
- utiliser uniquement des certificats à des fins légales et autorisées, conformément au CPS.
- demander une nouvelle carte pour étranger (et donc des certificats) en cas de changement des informations publiées dans le certificat;
- s'abstenir d'utiliser la clé publique dans un certificat délivré pour étranger, pour la délivrance d'autres certificats;
- utiliser un certificat de manière raisonnable en toutes circonstances;

- prévenir la compromission, la perte, la divulgation, la modification ou toute utilisation illicite de ses clés privées;
- avertir la police, l'administration communale ou le Helpdesk de la RA pour demander la suspension d'un certificat dans le cas où un incident portant matériellement atteinte à l'intégrité d'un certificat est suspecté. Ces incidents incluent des indications de perte, vol, modification, divulgation non autorisée ou autre compromission de la clé privée d'un des certificats, ou des deux;
- avertir la police, l'administration communale ou le Helpdesk de la RA pour demander la révocation d'un certificat dans le cas où un incident portant matériellement atteinte à l'intégrité d'un certificat. Ces incidents incluent la perte, le vol, la modification, la divulgation non autorisée ou la compromission de la clé privée d'un des certificats, ou des deux.
- n'utiliser sa paire de clés qu'en conformité avec toute limitation qui lui aura été notifiée;
- protéger sa clé privée à tout moment contre la perte, la divulgation à une autre partie, la modification et l'utilisation non autorisée, conformément au CPS en vigueur
- de notifier le Helpdesk RA sans délais dans le cas où le contrôle de la clé privée a été perdu suite à une compromission du code PIN.
- Dès compromission, l'obligation d'arrêter immédiatement et définitivement l'usage de la clé privée.

9.4.2 Obligations de la partie confiante

Les parties faisant confiance à un certificat du CSP :

- seront suffisamment informées sur l'utilisation de certificats numériques et PKI;
- seront informées et adhèreront aux conditions de ce CPS ainsi qu'aux conditions associées pour les parties confiantes;
- valideront un certificat en utilisant une validation de certificats basée CRL, delta CRL, OCSP ou Web, conformément à la procédure de validation du chemin du certificat;
- ne feront confiance à un certificat que s'il n'a pas été suspendu ou révoqué;
- feront confiance à un certificat de manière raisonnable en fonction des circonstances.

Les parties accédant aux informations reprises dans les dépôts ainsi que sur le site Web du CA sont seules responsables de l'évaluation de ces informations et du crédit qu'elles leur accordent.

Si une partie confiante prend connaissance de ou soupçonne la compromission d'une clé privée, elle avertira immédiatement le Helpdesk de la RA.

9.4.3 Responsabilité de l' étranger envers les parties confiantes

Tout étranger détenant une carte pour étranger avec des clés activées pour l'authentification et des signatures est responsable envers les parties confiantes pour toute utilisation de ladite carte, en ce compris des clés et certificats, sauf s'il peut prouver que sa clé a été compromise et qu'il a pris toutes les mesures nécessaires pour révoquer ses certificats dans les délais.

9.4.4 Conditions d'utilisation du centre de demande et du site Web

Les parties, comme les étrangers et les parties confiantes, qui accèdent au centre de demande et au site Web du CA sont d'accord avec les dispositions de ce CPS, ainsi qu'avec toutes les autres conditions d'utilisation. Les étrangers et les parties confiantes témoignent de leur acceptation des conditions d'utilisation et de ce CPS en introduisant une requête en rapport avec l'état d'un certificat numérique ou en ayant recours ou en faisant confiance, de quelque manière que ce soit, aux informations ou services fournis. Le centre de demande du CA peut être consulté de différentes manières :

- pour obtenir des informations résultant de la recherche d'un certificat numérique;

- pour vérifier le statut de signatures numériques créées avec une clé privée correspondant à une clé publique incluse dans un certificat;
- pour obtenir des informations publiées sur le site Web du CA;
- pour tous les autres services que le CA pourrait promouvoir ou fournir par l'intermédiaire de son site Web.

9.4.4.1 Confiance à ses propres risques et périls

Les parties accédant aux informations reprises au centre de demande ainsi que sur le site Web sont seules responsables de l'évaluation de ces informations et du crédit qu'elles leur accordent.

9.4.4.2 Précision des informations

Le CA met tout en oeuvre pour veiller à ce que les parties accédant au centre de demande reçoivent des informations précises, mises à jour et exactes. Le CSP, néanmoins, ne peut accepter une responsabilité au-delà des limites définies dans l'article 9.2. du CPS.

9.4.5 Obligations du CSP

Dans les limites de ce qui est spécifié dans les sections pertinentes du CPS, le CSP :

- se conformera au présent CPS et à ses amendements tels que publiés sous http://repository.eid.belgium.be;
- fournira des services d'infrastructure et de certification, notamment l'établissement et le fonctionnement du centre de demande et du site Web du CA pour le fonctionnement de services de certification publique;
- fournira des mécanismes de confiance, et notamment un mécanisme de génération de clés, une protection de clé ainsi que des procédures de partage de secret concernant sa propre infrastructure;
- avertira rapidement la RA en cas de compromission de sa (ses) propre(s) clé(s) privée(s);
- délivrera des certificats électroniques conformément au CPS et répondra à ses obligations telles que présentées dans le CPS;
- avertira la RA si le CA est incapable de valider l'application conformément à ce CPS;
- agira rapidement pour délivrer un certificat conformément à ce CPS, après avoir reçu une demande authentifiée de la RA;
- révoquera rapidement un certificat conformément au CPS, après avoir reçu une demande authentifiée de révocation de la part de la RA;
- suspendra rapidement un certificat conformément à la CPS, après avoir reçu une demande authentifiée de suspension de la part de la RA;
- lèvera rapidement la suspension d'un certificat conformément au CPS, après avoir reçu une demande authentifiée de levée de la suspension de la part de la RA;
- publiera des certificats conformément à ce CPS.
- Publiera les réponses CRL, delta CRL et OCSP de tous les certificats suspendus et révoqués, sur une base régulière, et conformément à ce CPS;
- fournira des niveaux de service appropriés selon un accord de niveau de service défini dans le cadre du contrat entre le CA et l'Autorité Fédérale Belge;
- fera une copie de ce CPS et des politiques en vigueur disponibles via son site Web;
- agira conformément aux lois belges. Concrètement, le CSP répondra à toutes les exigences légales associées à un profil de certificat qualifié émanant de la loi belge du 9 juillet 2001 sur les signatures électroniques, transposant la directive européenne 1999/93 sur un cadre communautaire pour les signatures électroniques.

Si le CSP prend connaissance ou soupçonne la compromission d'une clé privée, y compris la sienne, il avertira immédiatement la RA.

En cas de recours à des agents tiers, le CSP fera de son mieux pour garantir la responsabilité financière et civile adéquate dudit contractant.

Le CSP est, vis-à-vis des étrangers et des parties confiantes, responsable des actes ou omissions suivantes :

- la délivrance de certificats numériques ne reprenant pas les données telles que soumises par la RA;
- la compromission d'une clé de signature privée du CA;
- l'absence de révocation d'un certificat suspendu après une période d'une semaine;
- l'oubli de répertorier un certificat révoqué ou suspendu dans une CRL ou delta CRL;
- la non déclaration, par le répondeur OCSP, d'un certificat révoqué ou suspendu;
- la non déclaration, par une interface Web, d'informations sur le statut du certificat;
- la divulgation non autorisée d'informations confidentielles ou de données privées conformément aux sections 9.3 et 9.4.
- responsable comme définit en 9.2

Le CSP reconnaît qu'il n'a pas d'autres obligations dans le cadre de ce CPS.

9.4.6 Mesure du niveau de service

L'Autorité Fédérale Belge, avec ses partenaires eID, impose des contrôles destinés à garantir la conformité de services liés à l'eID avec les accords de niveau de service définis dans ce CPS.

9.4.7 Obligations de la RA (applicables au RRN)

La RA agissant dans le domaine du CA :

- fournira des informations correctes et précises dans ses communications avec le CA; • garantira que la clé publique soumise au CA correspond à la clé privée utilisée;
- créera des demandes de certificats conformément à ce CPS.
- procédera à toutes les vérifications et authentifications prescrites par les procédures du CA et ce CPS;
- soumettra la demande du requérant au CA, dans un message signé;
- recevra, vérifiera et transmettra au CA toutes les demandes de révocation, suspension et réhabilitation après suspension d'un certificat conformément aux procédures du CA et au CPS;
- vérifiera l'exactitude et l'authenticité des informations fournies par l'étranger au moment du renouvellement d'un certificat conformément à ce CPS.

Si la RA prend connaissance de ou soupçonne la compromission d'une clé privée, elle informera immédiatement le CA.

RRN agit comme unique RA dans le domaine du CA, tout en ayant toutefois le droit de sousdéléguer l'enregistrement aux LRA, comme les administrations communales.

La RA est seule responsable des répertoires qu'elle tient à jour, y compris des répertoires de certificats.

La RA est responsable de tous les audits qu'elle effectue, ainsi que des résultats et recommandations de tels audits.

La RA, par l'intermédiaire de la LRA, est seule responsable de l'exactitude des données de l' étranger ainsi que de toute autre donnée cédée qu'elle fournit au CA. La RA et non le CA est responsable de tous les dommages encourus à la suite de données non vérifiées qui ont été reprises dans un certificat.

La RA se conforme aux lois et règlements belges relatifs au fonctionnement de RRN.
La RA est responsable de ses actes ou omissions, conformément à la loi belge.

9.4.8 Obligations du personnalisateur et de l'initialisateur (CM)

Le producteur des cartes pour étrangers (CM) est responsable de l'initialisation, de la personnalisation et de la distribution des cartes pour étrangers contenant des deux certificats

L'initialisation comprend les opérations suivantes dans la puce :

- La génération des trois paires de clés,
- Le stockage des données d'identification et des certificats,
- L'authentification des données, ainsi que l'initialisation des différents fichiers.

Le CM distribuera en toute sécurité les documents de base, les lettres de convocation, les nouvelles cartes pour étrangers personnalisées et initialisées, ainsi que les lettres sécurisées personnalisées destinées aux étrangers et qui contiennent les codes PIN et PUK1.

La réalisation d'un système sécurisé pour la collecte dans les administrations communales des cartes échues ou annulées et leur destruction.

9.5 Dégagements de garantie

Cette section comprend des dégagements de garantie expresse.

9.5.1 Exclusion de certains éléments de préjudices

Dans la limite fixée par la loi belge, le CSP ne sera en aucun cas (sauf en cas de fraude ou d'inconduite délibérée) responsable pour :

- la perte de profits;
- la perte de données;
- tous préjudices indirects, consécutifs ou dissuasifs découlant de ou en rapport avec l'utilisation, la livraison, la licence et l'exécution ou la non-exécution de certificats ou signatures numériques;
- tout autre préjudice.

9.6 Durée et résiliation

Le présent CPS reste d'application jusqu'à ce le CSP stipule le contraire dans ses archives de référence, sous le site http://repository.eid.belgium.be .
Les changements notifiés sont marqués comme il se doit par une version indiquée.

9.7 Remarques individuelles et communications avec les participants

Les remarques relatives à ce CPS peuvent être adressées au : CSP pour le “Foreigner CA” p/a CERTIPOST, Centre Monnaie, 1000 Bruxelles.

9.8 Clause contraignante

Si une des dispositions du présent CPS, s’avère être invalide ou non applicable, les autres dispositions de ce CPS seront interprétées de manière à respecter l’intention originale des parties.

9.9 Amendements

Les changements mineurs apportés au présent CPS et qui n’affectent pas matériellement le niveau de garantie de ce CPS sont indiqués par un numéro de version comprenant un nombre décimal (ex. version 1.0 deviens version 1.1), tandis que une version comportant des changements majeurs est indiqué par un numéro complet (ex. version 1.0 deviens version 2.0).

Les changements mineurs apportés à ce CPS ne requièrent aucun changement dans le CPS OID ou au niveau du pointeur vers le CPS (URL) qui pourrait être communiqué par le CSP. Les changements majeurs susceptibles de modifier matériellement l’acceptabilité de certificats destinés à des fins spécifiques peuvent requérir des changements adaptés au niveau du CPS OID ou du pointeur vers le CPS (URL).

9.10 Procédures de résolution des litiges

Tous les litiges associés au présent CPS seront réglés conformément à la loi belge.

9.11 Droit applicable

Le CSP fournit ses services conformément aux dispositions de la loi belge.

9.12 Dispositions diverses

Le CSP incorpore par référence les informations suivantes dans tous les certificats numériques qu’il délivre :

- les termes et conditions décrits dans le présent CPS;
- toute autre politique de certificat applicable, telle qu’elle peut être précisée sur un certificat de l’étranger délivré;
- les éléments obligatoires des normes applicables;
- les éléments non obligatoires mais personnalisés des normes applicables;
- le contenu d’extensions et la dénomination améliorée non abordée ailleurs; • Toute autre information indiquée comme telle dans un champ d’un certificat.

Pour incorporer par référence des informations, le CA utilise des pointeurs basés sur un ordinateur ou sur du texte et incluant des URL, OID, etc.

10. Liste de définitions

Accréditation	Déclaration formelle, par une autorité approbatrice, selon laquelle une fonction / entité donnée répond à des exigences formelles spécifiques.
Authority Information Access (AIA)	Champ d'information repris comme extension dans le certificat pour établir automatiquement le chemin en vue de vérifier la hiérarchie de confiance dans les applications les plus générales, comme les navigateurs.
Archive	Utilisée pour conserver des enregistrements pendant une période donnée, à des fins de sécurité, de sauvegarde ou de vérification.
Centre de demande	Base de données et/ou répertoire reprenant les certificats numériques et d'autres informations pertinentes accessibles en ligne.
Audit	Procédure utilisée pour valider la conformité avec des critères ou contrôles formels.
Authentification	Processus mis en oeuvre pour confirmer l'identité d'une personne ou prouver l'intégrité d'informations spécifiques en les plaçant dans le bon contexte et en vérifiant la relation.
Autorité d'enregistrement locale ou LRA	Une LRA est une entité (organisation) agissant sur délégation d'une RA pour enregistrer des demandes de certificats numériques. La LRA est chargée d'enregistrer d'autres entités et de leur attribuer une valeur de distinction relative comme un nom distinctif ou une condensation d'un certificat univoque faisant partie de ce domaine.
Autorité d'enregistrement ou RA	Entité chargée d'identifier et d'authentifier des étrangers. La RA ne délivre pas de certificats. Dans le domaine du CA, RRN est la RA.
Autorité de certification ou CC	Autorité chargée d'associer une clé publique aux informations sur la personne concernée reprises dans le certificat, en signant ce dernier avec sa clé privée. Sauf mention explicite, le CA décrit ici est le 'Foreigner Certification Authority'.
Certificat	Déclaration électronique qui associe les données de vérification de la signature à une personne physique ou morale et confirme l'identité de cette personne.
Certificat normalise	Certificat utilisé pour supporter n'importe quel usage sauf des signatures électroniques qualifiées d'une paire de clés cryptographiques dont la paire de clés publiques correspondante est certifiée. Les usages de clés certifiées peuvent consister en un ou plusieurs des usages suivants : chiffrement, authentification, signatures non qualifiées, etc. Le certificat normalisé est délivré conformément aux exigences de la norme technique TS 102 042 de l'ETSI.

Certificat qualifie	Certificat utilisé exclusivement pour supporter une signature électronique, conforme aux exigences de l'annexe I de la directive européenne 1999/93 et délivré par un fournisseur de services de certification répondant aux conditions de l'annexe II de la directive européenne 1999/93, en mentionnant la loi belge du 09 juillet 2001, la norme technique ETS TS 101 456, les normes techniques ETSI TS "profil de certificat qualifié" et la norme RFC 3039 "Infrastructure à clés publiques Internet X 509 et profil de certificat qualifié"
Certificat suspendu	Certificat temporairement rejeté mais néanmoins conservé pendant une semaine, jusqu'à ce qu'un avis de révocation ou de réhabilitation soit délivré au CA par RRN
Chaîne de certificats	Liste hiérarchique de certificats comprenant un certificat d'utilisateur final et des certificats du CA.
Clé privée	Clé mathématique utilisée pour créer des signatures numériques et, parfois (selon l'algorithme), décrypter messages en combinaison avec la clé publique correspondante.
Clé publique	Clé mathématique pouvant être mise à la disposition du public et utilisée pour vérifier des signatures générées à l'aide de la clé privée correspondante. Selon l'algorithme, les clés publiques peuvent aussi servir à crypter messages ou fichiers qui seront ensuite décryptés avec la clé privée correspondante.
Confiance	Le fait d'accepter une signature numérique et d'agir de manière à montrer sa foi en ladite signature.
Confidentialité	Condition de divulgation de données à des parties sélectionnées et autorisées uniquement.
Cryptographie a clés publiques	Cryptographie reposant sur une paire de clés cryptographiques mathématiquement apparentées.
Délivrance de certificats	Délivrance de certificats numériques X.509 v3 destinés à l'identification et à la signature digitale à partir de données à caractère personnel et de clés publiques fournies par la RA et conformes au CPS.
Détenteur de part de secret	Personne qui détient une part de secret.
Directive européenne	La directive européenne 1999/93 du Parlement européen et du Conseil du 13 décembre 1999 "sur un cadre communautaire pour les signatures électroniques''.
eID	L'intégralité du système de la carte d'identité électronique, notamment l'organisation, l'infrastructure, les procédures, les contacts et toutes les ressources nécessaires, relatifs à la carte d'identité.
Emetteur d'une part de secret	Personne créant et distribuant des parts de secret, et notamment un CA
Enonce des pratiques de certification ou CPS	Enoncé des pratiques de gestion de certificats pendant toutes les phases du cycle de vie des certificats.
Expiration du certificat	La fin de la période de validité d'un certificat numérique.
Extension du certificat	Un champ du certificat numérique utilisé pour transmettre des informations supplémentaires sur des domaines comme : la clé publique, l'étranger certifié, l'émetteur du certificat, et / ou le processus de certification.
Génération d'une paire de clés	Processus fiable destiné à créer des clés privées et publiques liées mathématiquement (ex. : selon l'algorithme RSA).

Gestion de certificats	Actions associées à la gestion de certificats, comme le stockage, la diffusion, la publication, la révocation et la suspension de certificats
Hiérarchie de certificat	Une séquence sur plusieurs niveaux de certificats d'un CA (racine) et d'entités subordonnées comme des autorités de certification et des étrangers.
Hiérarchie des PKI	Ensemble d'autorités de certification dont les fonctions sont organisées selon le principe de la délégation d'autorité et reliées les unes aux autres en tant que CA subordonné et supérieur.
HSM	Un HSM (Hardware Security Module) est un composant de sécurité hardware qui génère des clés cryptographiques, stocke et protège.
Identificateur d'objets (OID)	Une séquence de composantes intègres peut être attribuée à un objet enregistré et cette séquence a la particularité d'être unique parmi tous les identificateurs d'objets d'un domaine spécifique.
Incorporer par référence	Pour intégrer un document dans un autre en identifiant le document à incorporer, avec des informations permettant au bénéficiaire d'accéder et d'obtenir le message incorporé dans son intégralité, et en exprimant l'intention que ce document fasse partie du message incorporant. Un tel message incorporé devrait avoir le même effet que s'il était à part entière du message.
Infrastructure a clés publiques (PKI)	Architecture, organisation, techniques, pratiques et procédures qui supportent collectivement l'installation et l'opération d'un système de chiffrement à clé publique basé sur un certificat.
Liste de révocation de certificats (CRL)	Liste délivrée et signée numériquement par un CA et qui comprend des certificats révoqués ou suspendus. Cette liste peut être consultée à tout moment par les parties confiantes, avant de faire confiance aux informations reprises dans un certificat.
Nom distinctif	Ensemble de données identifiant une entité du monde réel, telle qu'une personne dans un contexte informatique.
Numéro de série d'un Certificat	Numéro séquentiel identifiant de façon unique un certificat dans le domaine d'un CA.
Paire de clés	Une clé privée et sa clé publique correspondante, dans un chiffrement asymétrique.
Partage de secret	Partie d'un secret cryptographique divisée en plusieurs jetons physiques, comme des cartes à puces, etc.
Partie confiante	Toute entité qui fait confiance à un certificat pour agir.
Position de confiance	Un rôle qui, au sein d'un CA, comprend l'accès à ou le contrôle d'opérations cryptographiques pouvant justifier un accès privilégié à la délivrance, l'utilisation, la suspension ou la révocation de certificats, en ce compris l'accès à ou le contrôle d'opérations limitant l'accès à des archives de référence.
Protocole de vérification d'état De Certificat En Ligne (OCSP)	Le protocole de vérification d'état de certificat en ligne (RFC 2560) est une source d'informations sur l'état en temps réel utilisée pour déterminer le statut actuel d'un certificat numérique sans que des CRL soient nécessaires.
Remarque	Résultat de la notification à des parties impliquées dans la réception de services CA conformément à ce CPS
Révocation de certificats	Service en ligne utilisé pour désactiver un certificat numérique en permanence avant sa date d'expiration.

Révoquer un certificat	Mettre définitivement fin à la période de validité d'un certificat, à partir d'un moment spécifié.
Service d'état De Certificats	Service permettant à des parties confiantes et à d'autres de vérifier l'état de certificats.
Services de certification	Services relatifs au cycle de vie des certificats. Les services de certification sont des services publics.
Signataire	Personne qui commande l'appareil de création de signatures utilisé pour générer une signature numérique.
Signature	Méthode utilisée ou adoptée par l'auteur d'un document pour s'identifier. Cette méthode peut être acceptée par le destinataire ou son utilisation est habituelle dans les circonstances données.
Signature digitale	Sert à encoder un message à l'aide d'un système de chiffrement asymétrique et une fonction de condensation de telle sorte qu'une personne détenant le message initial et la clé publique du signataire puisse savoir avec précision si la transformation a été effectuée à l'aide de la clé privée correspondant à la clé publique du signataire et si le message initial a été modifié depuis la transformation.
Signature électronique	Données électroniques attachées ou liées logiquement à d'autres données électroniques et activant la méthode d'authentification.
Signature racine (root signing)	Acte par lequel une autorité supérieure sur le plan hiérarchique octroie, sous condition, son statut de confiance à une autorité inférieure. Dans le contexte de la carte pour étranger, digicert cybertrust global est une autorité de root sign autorisant le CA à bénéficier du même statut de confiance dans des applications logicielles, comme les propres certificats dedigicert cybertrust global.
Souscripteur	Personne dont l'identité et la clé publique sont certifiées dans des certificats.
Suspension de certificats	Service en ligne utilisé pour désactiver provisoirement un certificat numérique et le révoquer automatiquement si aucune demande de réhabilitation n'est présentée dans un certain délai.
Système fiable	Matériel informatique, logiciels et procédures offrant un niveau de protection acceptable contre les risques liés à la sécurité, offrant un niveau de disponibilité et de fiabilité suffisant, fonctionnant correctement et mettant en œuvre une politique de sécurité.
Valider une chaîne de certificats	Valider une chaîne de certificats pour valider chaque certificat de la chaîne de certificats de manière à valider un certificat utilisateur final.
Vérification d'état	Service en ligne basé, par exemple, sur le protocole de vérification d'état de certificat en ligne (RFC 2560) et utilisé pour déterminer l'état actuel d'un certificat numérique sans que des CRL soient nécessaires. Plusieurs mécanismes de vérification d'état sont mis à disposition par l'infrastructure eID, comme des interfaces CRL, delta CRL, OCSP et Web.
X.509	La norme de la ITU-T (International Telecommunications Union-T) en matière de certificats numériques.

11. Liste d'acronymes

BRCA	Belgium Root CA	CA racine pour la Belgique
CA	Certification Authority	Autorité de certification
CM	Card Manufacturer	Producteur de cartes
CPS	Certificate Practise Statement	Enoncé des pratiques de certification
CRL	Certificate Revocation List	Liste de révocation de certificats
HSM	Hardware Security Module	Module de sécurité hardware
LRA	Local Registration Authority	Autorité d'enregistrement locale
OID	Object Identifier	Identificateur d'objets
OCSP	Online Certificate Status Protocol	Protocole de vérification de l'état du certificat en ligne
PKI	Public Key Infrastructure	Infrastructure à clés publiques
RA	Registration Authority	Autorité d'enregistrement
SRA	Suspension and Revocation Authority	Autorité de suspension et de révocation
OID	Object Identifier	identificateur d'objet
URL	Uniform Resource Locator	Indicateur d'adresse Internet
PIN	Personal Identification Number	Code d'identification personnel
PUK	Personal Unblocking Key	Code de déblocage personnel